



CISM.examlabs.premium.exam.1154q

CISM

CISM

Certified Information Security Manager

Version 9.0

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (1154 questions)

Question 1

Following a recent acquisition, an information security manager has been requested to address the outstanding risk reported early in the acquisition process. Which of the following would be the manager's BEST course of action?

- ☐ Add the outstanding risk to the acquiring organization's risk registry.
- ☐ Re-assess the outstanding risk of the acquired company.
- ☐ Re-evaluate the risk treatment plan for the outstanding risk.
- ☐ Perform a vulnerability assessment of the acquired company's infrastructure.

Question 2

It is suspected that key e-mails have been viewed by unauthorized parties. The e-mail administrator conducted an investigation but it has not returned any information relating to the incident, and leaks are continuing. Which of the following is the BEST recommended course of action to senior management?

- ☐ Commence security training for staff at the organization.
- ☐ Arrange for an independent review.
- ☐ Rebuild the e-mail application.
- ☐ Restrict the distribution of confidential e-mails.

Question 3

Which of the following would raise security awareness among an organization's employees?

- ☐ Distributing industry statistics about security incidents
- ☐ Monitoring the magnitude of incidents
- ☐ Encouraging employees to behave in a more conscious manner
- ☐ Continually reinforcing the security policy

Question 4

Which of the following is the BEST way for information security manager to identify compliance with information security policies within an organization?

- ☐ Analyze system logs.
- ☐ Conduct security awareness testing.
- ☐ Perform vulnerability assessments.
- ☐ Conduct periodic audits.

Question 5

There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

- ☐ Identify the vulnerable systems and apply compensating controls
- ☐ Minimize the use of vulnerable systems
- ☐ Communicate the vulnerability to system users
- ☐ Update the signatures database of the intrusion detection system (IDS)

Question 6

In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

- ☐ Procedural design
- ☐ Architectural design
- ☐ System design specifications
- ☐ Software development

Question 7

An organization with multiple data centers has designated one of its own facilities as the recovery site. The MOST important concern is the:

- ☐ communication line capacity between data centers.
- ☐ current processing capacity loads at data centers.
- ☐ differences in logical security at each center.
- ☐ synchronization of system software release versions.

Question 8

When outsourcing data to a cloud service provider, which of the following should be the information security manager's MOST important consideration?

- ☐ Roles and responsibilities have been defined for the subscriber organization.
- ☐ Cloud servers are located in the same country as the organization.
- ☐ Access authorization includes biometric security verification.
- ☐ Data stored at the cloud service provider is not co-mingled.

Question 9

A validated patch to address a new vulnerability that may affect a mission-critical server has been released.

What should be done immediately?

- ☐ Add mitigating controls.
- ☐ Check the server's security and install the patch.
- ☐ Conduct an impact analysis.
- ☐ Take the server off-line and install the patch.

Question 10

For an organization that is experiencing outages due to malicious code, which of the following is the BEST index of the effectiveness of countermeasures?

- ☐ Number of virus infections detected
- ☐ Amount of infection-related downtime
- ☐ Average recovery time per incident
- ☐ Number of downtime-related help desk calls

Question 11

Which of the following is MOST important for an information security manager to communicate to senior management regarding the security program?

- ☐ Potential risks and exposures
- ☐ Impact analysis results
- ☐ Security architecture changes
- ☐ User roles and responsibilities

Question 12

A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

- ☐ User
- ☐ Network
- ☐ Operations
- ☐ Database

Question 13

The implementation of continuous monitoring controls is the BEST option where:

- ☐ incidents may have a high impact and frequency
- ☐ legislation requires strong information security controls
- ☐ incidents may have a high impact but low frequency
- ☐ Electronic commerce is a primary business driver

Question 14

The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

- ☐ generally accepted industry best practices.
- ☐ business requirements.
- ☐ legislative and regulatory requirements.
- ☐ storage availability.

Question 15

A penetration test was conducted by an accredited third party. Which of the following should be the information security manager's FIRST course of action?

- ☐ Ensure vulnerabilities found are resolved within acceptable timeframes.
- ☐ Request funding needed to resolve the top vulnerabilities.
- ☐ Report findings to senior management.
- ☐ Ensure a risk assessment is performed to evaluate the findings.

Question 16

What does a network vulnerability assessment intend to identify?

- ☐ 0-day vulnerabilities
- ☐ Malicious software and spyware
- ☐ Security design flaws
- ☐ Misconfiguration and missing updates

Question 17

What is the PRIMARY goal of an incident management program?

- ☐ Minimize impact to the organization.
- ☐ Contain the incident.
- ☐ Identify root cause.
- ☐ Communicate to external entities.

Question 18

An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

- ☐ mitigate the impact by purchasing insurance.
- ☐ implement a circuit-level firewall to protect the network.
- ☐ increase the resiliency of security measures in place.
- ☐ implement a real-time intrusion detection system.

Question 19

Which of the following is the MOST important to ensure a successful recovery?

- ☐ Backup media is stored offsite
- ☐ Recovery location is secure and accessible
- ☐ More than one hot site is available
- ☐ Network alternate links are regularly tested

Question 20

Which of the following is the BEST reason to perform a business impact analysis (BIA)?

- ☐ To help determine the current state of risk
- ☐ To budget appropriately for needed controls
- ☐ To satisfy regulatory requirements
- ☐ To analyze the effect on the business

Question 21

Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

- ☐ Reconciliation of the annual systems inventory to the disaster recovery, business continuity plans
- ☐ Periodic audits of the disaster recovery/business continuity plans
- ☐ Comprehensive walk-through testing
- ☐ Inclusion as a required step in the system life cycle process

Question 22

Which of the following presents the GREATEST challenge in calculating return on investment (ROI) in the security environment?

- ☐ Number of incidents cannot be predetermined
- ☐ Project cost overruns cannot be anticipated
- ☐ Cost of security tools is difficult to estimate
- ☐ Costs of security incidents cannot be estimated

Question 23

The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

- ☐ change the root password of the system.
- ☐ implement multifactor authentication.
- ☐ rebuild the system from the original installation medium.
- ☐ disconnect the mail server from the network.

Question 24

Senior management commitment and support for information security can BEST be enhanced through:

- ☐ a formal security policy sponsored by the chief executive officer (CEO).
- ☐ regular security awareness training for employees.
- ☐ periodic review of alignment with business management goals.
- ☐ senior management signoff on the information security strategy.

Question 25

An information security steering group should:

- ☐ provide general oversight and guidance.
- ☐ develop information security policies.
- ☐ establish information security baselines.
- ☐ oversee the daily operations of the security program.

Question 26

Which of the following would BEST help to ensure an organization's security program is aligned with business objectives?

- ☐ Security policies are reviewed and approved by the chief information officer.
- ☐ The security strategy is reviewed and approved by the organization's executive committee.
- ☐ The organization's board of directors includes a dedicated information security specialist.
- ☐ Project managers receive annual information security awareness training.

Question 27

Security policies should be aligned MOST closely with:

- ☐ industry' best practices.
- ☐ organizational needs.
- ☐ generally accepted standards.
- ☐ local laws and regulations.

Question 28

Which of the following is MOST important to understand when developing a meaningful information security strategy?

- ☐ Regulatory environment
- ☐ International security standards
- ☐ Organizational risks
- ☐ Organizational goals

Question 29

In the course of examining a computer system for forensic evidence, data on the suspect media were inadvertently altered. Which of the following should have been the FIRST course of action in the investigative process?

- ☐ Perform a backup of the suspect media to new media.
- ☐ Perform a bit-by-bit image of the original media source onto new media.
- ☐ Make a copy of all files that are relevant to the investigation.
- ☐ Run an error-checking program on all logical drives to ensure that there are no disk errors.

Question 30

Which of the following would BEST address the risk of data leakage?

- ☐ File backup procedures
- ☐ Database integrity checks
- ☐ Acceptable use policies
- ☐ Incident response procedures

Question 31

The PRIMARY purpose for continuous monitoring of security controls is to ensure:

- ☐ system availability.
- ☐ control gaps are minimized.
- ☐ effectiveness of controls.
- ☐ alignment with compliance requirements.

Question 32

The PRIMARY objective of security awareness is to:

- ☐ ensure that security policies are understood.
- ☐ influence employee behavior.
- ☐ ensure legal and regulatory compliance
- ☐ notify of actions for noncompliance.

Question 33

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- ☐ User management coordination does not exist.
- ☐ Specific user accountability cannot be established.
- ☐ Unauthorized users may have access to originate, modify or delete data.
- ☐ Audit recommendations may not be implemented.

Question 34

Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

- ☐ Key control monitoring
- ☐ A robust security awareness program
- ☐ A security program that enables business activities
- ☐ An effective security architecture

Question 35

In which of the following ways can an information security manager BEST ensure that security controls are adequate for supporting business goals and objectives?

- ☐ Reviewing results of the annual company external audit
- ☐ Adopting internationally accepted controls
- ☐ Enforcing strict disciplinary procedures in case of noncompliance
- ☐ Using the risk management process

Question 36

Reviewing which of the following would provide the GREATEST input to the asset classification process?

- ☐ Risk assessment
- ☐ Replacement cost of the asset
- ☐ Sensitivity of the data
- ☐ Compliance requirements

Question 37

Security governance is MOST associated with which of the following IT infrastructure components?

- ☐ Network
- ☐ Application
- ☐ Platform
- ☐ Process

Question 38

Which of the following results from the risk assessment process would BEST assist risk management decision making?

- ☐ Control risk
- ☐ Inherent risk
- ☐ Risk exposure
- ☐ Residual risk

Question 39

Which of the following is the MOST important reason for performing a risk analysis?

- ☐ Assigning the appropriate level of protection
- ☐ Identifying critical information assets
- ☐ Identifying and eliminating threats
- ☐ Promoting increased security awareness in the organization

Question 40

Which of the following is the MOST usable deliverable of an information security risk analysis?

- ☐ Business impact analysis (BIA) report
- ☐ List of action items to mitigate risk
- ☐ Assignment of risks to process owners
- ☐ Quantification of organizational risk

Question 41

Which of the following documents would be the BEST reference to determine whether access control mechanisms are appropriate for a critical application?

- ☐ User security procedures
- ☐ Business process flow
- ☐ IT security policy
- ☐ Regulatory requirements

Question 42

Which of the following would help management determine the resources needed to mitigate a risk to the organization?

- ☐ Risk analysis process
- ☐ Business impact analysis (BIA)
- ☐ Risk management balanced scorecard
- ☐ Risk-based audit program

Question 43

The MOST important reason for conducting periodic risk assessments is because:

- ☐ risk assessments are not always precise.
- ☐ security risks are subject to frequent change.
- ☐ reviewers can optimize and reduce the cost of controls.
- ☐ it demonstrates to senior management that the security function can add value.

Question 44

Which of the following application systems should have the shortest recovery time objective (RTO)?

- ☐ Contractor payroll
- ☐ Change management
- ☐ E-commerce web site
- ☐ Fixed asset system

Question 45

The MOST effective use of a risk register is to:

- ☐ identify risks and assign roles and responsibilities for mitigation.
- ☐ identify threats and probabilities.
- ☐ facilitate a thorough review of all IT-related risks on a periodic basis.
- ☐ record the annualized financial amount of expected losses due to risks.

Question 46

It is important to classify and determine relative sensitivity of assets to ensure that:

- ☐ cost of protection is in proportion to sensitivity.
- ☐ highly sensitive assets are protected.
- ☐ cost of controls is minimized.
- ☐ countermeasures are proportional to risk.

Question 47

An information security manager has completed a risk assessment and has determined the residual risk. Which of the following should be the NEXT step?

- ☐ Conduct an evaluation of controls
- ☐ Determine if the risk is within the risk appetite
- ☐ Implement countermeasures to mitigate risk
- ☐ Classify all identified risks

Question 48

Reviewing security objectives and ensuring the integration of security across business units is PRIMARILY the focus of the:

- ☐ executive management
- ☐ chief information security officer (CISO)
- ☐ board of directors
- ☐ steering committee.

Question 49

Which of the following is MOST important to the success of an information security program?

- ☐ Security' awareness training
- ☐ Achievable goals and objectives
- ☐ Senior management sponsorship
- ☐ Adequate start-up budget and staffing

Question 50

When a business-critical web server is compromised, the IT security department should FIRST:

- ☐ archive the logs as evidence.
- ☐ attempt to repair any damage in order to keep the server running.
- ☐ notify the legal department and/or regulatory officials as required.
- ☐ advise management of the incident.

Question 51

Which of the following requirements would have the lowest level of priority in information security?

- ☐ Technical
- ☐ Regulatory
- ☐ Privacy
- ☐ Business

Question 52

When an information security manager presents an information security program status report to senior management, the MAIN focus should be:

- ☐ critical risks indicators.
- ☐ key controls evaluation.
- ☐ key performance indicators (KPIs).
- ☐ net present value (NPV).

Question 53

An extranet server should be placed:

- ☐ outside the firewall.
- ☐ on the firewall server.
- ☐ on a screened subnet.
- ☐ on the external router.

Question 54

In a social engineering scenario, which of the following will MOST likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

- ☐ Implementing on-screen masking of passwords
- ☐ Conducting periodic security awareness programs
- ☐ Increasing the frequency of password changes
- ☐ Requiring that passwords be kept strictly confidential

Question 55

When an organization and its IT-hosting service provider are establishing a contract with each other, it is MOST important that the contract includes:

- ☐ details of expected security metrics.
- ☐ each party's security responsibilities.
- ☐ penalties for noncompliance with security policy.
- ☐ recovery time objectives (RTOs).

Question 56

When residual risk is minimized:

- ☐ acceptable risk is probable.
- ☐ transferred risk is acceptable.
- ☐ control risk is reduced.
- ☐ risk is transferable.

Question 57

Phishing is BEST mitigated by which of the following?

- ☐ Security monitoring software
- ☐ Encryption
- ☐ Two-factor authentication
- ☐ User awareness

Question 58

The authorization to transfer the handling of an internal security incident to a third-party support provider is PRIMARILY defined by the:

- ☐ information security manager
- ☐ escalation procedures
- ☐ disaster recovery plan
- ☐ chain of custody

Question 59

Which of the following could be detected by a network intrusion detection system (IDS)?

- ☐ Undocumented open ports
- ☐ Unauthorized file change
- ☐ Internally generated attacks
- ☐ Emailed virus attachments

Question 60

The FIRST priority when responding to a major security incident is:

- ☐ documentation.
- ☐ monitoring.
- ☐ restoration.
- ☐ containment.

Question 61

Which of the following should be of MOST concern to an information security manager reviewing an organization's data classification program?

- ☐ The program allows exceptions to be granted.
- ☐ Labeling is not consistent throughout the organization.
- ☐ Data retention requirements are not defined.
- ☐ The classifications do not follow industry best practices.

Question 62

Internal audit has reported a number of information security issues which are not in compliance with regulatory requirements. What should the information security manager do FIRST?

- ☐ Create a security exception
- ☐ Perform a vulnerability assessment
- ☐ Perform a gap analysis to determine needed resources
- ☐ Assess the risk to business operations

Question 63

The BEST time to ensure that a corporation acquires secure software products when outsourcing software development is during:

- ☐ corporate security reviews.
- ☐ contract performance audits.
- ☐ contract negotiation.
- ☐ security policy development.

Question 64

An organization's information security processes are currently defined as ad hoc. In seeking to improve their performance level, the next step for the organization should be to:

- ☐ ensure that security processes are consistent across the organization.
- ☐ enforce baseline security levels across the organization.
- ☐ ensure that security processes are fully documented.
- ☐ implement monitoring of key performance indicators for security processes.

Question 65

Investments in information security technologies should be based on:

- ☐ vulnerability assessments.
- ☐ value analysis.
- ☐ business climate.
- ☐ audit recommendations.

Question 66

Which of the following is an example of a vulnerability?

- ☐ Natural disasters
- ☐ Defective software
- ☐ Ransomware
- ☐ Unauthorized users

Question 67

The risk of mishandling alerts identified by an intrusion detection system (IDS) would be the GREATEST when:

- ☐ standard operating procedures are not formalized
- ☐ the IT infrastructure is diverse
- ☐ IDS sensors are misconfigured.
- ☐ operations and monitoring are handled by different teams.

Question 68

Which of the following is a risk of cross-training?

- ☐ Increases the dependence on one employee
- ☐ Does not assist in succession planning
- ☐ One employee may know all parts of a system
- ☐ Does not help in achieving a continuity of operations

Question 69

A risk assessment should be conducted:

- ☐ once a year for each business process and subprocess.
- ☐ every three to six months for critical business processes.
- ☐ by external parties to maintain objectivity.
- ☐ annually or whenever there is a significant change.

Question 70

The valuation of IT assets should be performed by:

- ☐ an IT security manager.
- ☐ an independent security consultant.
- ☐ the chief financial officer (CFO).
- ☐ the information owner.

Question 71

Identification and prioritization of business risk enables project managers to:

- ☐ establish implementation milestones.
- ☐ reduce the overall amount of slack time.
- ☐ address areas with most significance.
- ☐ accelerate completion of critical paths.

Question 72

The PRIMARY advantage of involving end users in continuity planning is that they:

- ☐ are more objective than information security management.
- ☐ can balance the technical and business risks.
- ☐ have a better understanding of specific business needs.
- ☐ can see the overall impact to the business.

Question 73

Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

- ☐ are compatible with the provider's own classification.
- ☐ are communicated to the provider.
- ☐ exceed those of the outsourcer.
- ☐ are stated in the contract.

Question 74

A new version of an information security regulation is published that requires an organization's compliance. The information security manager should FIRST:

- ☐ perform an audit based on the new version of the regulation.
- ☐ conduct a risk assessment to determine the risk of noncompliance.
- ☐ conduct benchmarking against similar organizations.
- ☐ perform a gap analysis against the new regulation.

Question 75

Which of the following should occur FIRST in the process of managing security risk associated with the transfer of data from unsupported legacy systems to supported systems?

- ☐ Make backups of the affected systems prior to transfer.
- ☐ Increase cyber insurance coverage.
- ☐ Identify all information assets in the legacy environment.
- ☐ Assign owners to be responsible for the transfer of each asset.

Question 76

An information security manager is analyzing a risk that is believed to be severe, but lacks numerical evidence to determine the impact the risk could have on the organization. In this case the information security manager should:

- ☐ use a qualitative method to assess the risk.
- ☐ use a quantitative method to assess the risk.
- ☐ put it in the priority list in order to gain time to collect more data.
- ☐ ask management to increase staff in order to collect more evidence on severity.

Question 77

The department head of application development has decided to accept the risks identified in a recent assessment. No recommendations will be implemented, even though the recommendations are required by regulatory oversight. What should the information security manager do NEXT?

- ☐ Formally document the decision.
- ☐ Review the risk monitoring plan.
- ☐ Perform a risk reassessment.
- ☐ Implement the recommendations.

Question 78

An information security manager wishing to establish security baselines would:

- ☐ include appropriate measurements in the system development life cycle.
- ☐ implement the security baselines to establish information security best practices.
- ☐ implement the security baselines to fulfill laws and applicable regulations in different jurisdictions.
- ☐ leverage information security as a competitive advantage.

Question 79

To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

- ☐ end users.
- ☐ legal counsel.
- ☐ operational units.
- ☐ audit management.

Question 80

What would be the MOST significant security risks when using wireless local area network (LAN) technology?

- ☐ Man-in-the-middle attack
- ☐ Spoofing of data packets
- ☐ Rogue access point
- ☐ Session hijacking

Question 81

Which of the following techniques would be the BEST test of security effectiveness?

- ☐ Performing an external penetration test
- ☐ Reviewing security policies and standards
- ☐ Reviewing security logs
- ☐ Analyzing technical security practices

Question 82

Which of the following provides the BKST confirmation that the business continuity/disaster recovery plan objectives have been achieved?

- ☐ The recovery time objective (RTO) was not exceeded during testing
- ☐ Objective testing of the business continuity/disaster recovery plan has been carried out consistently
- ☐ The recovery point objective (RPO) was proved inadequate by disaster recovery plan testing
- ☐ Information assets have been valued and assigned to owners per the business continuity plan, disaster recovery plan

Question 83

After the occurrence of a major information security incident, which of the following will BEST help an information security manager determine corrective actions?

- ☐ Calculating cost of the incident
- ☐ Conducting a postmortem assessment
- ☐ Preserving the evidence
- ☐ Performing an impact analysis

Question 84

Which of the following is the FIRST step to perform before outsourcing critical information processing to a third party?

- ☐ Require background checks for third-party employees.
- ☐ Perform a risk assessment.
- ☐ Ensure that risks are formally accepted by third party.
- ☐ Negotiate a service level agreement.

Question 85

Which of the following should be the PRIMARY goal of an information security manager when designing information security policies?

- ☐ Reducing organizational security risk
- ☐ Improving the protection of information
- ☐ Minimizing the cost of security controls
- ☐ Achieving organizational objectives

Question 86

An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the following should the organization do FIRST?

- ☐ Request that the third-party provider perform background checks on their employees.
- ☐ Perform an internal risk assessment to determine needed controls.
- ☐ Audit the third-party provider to evaluate their security controls.
- ☐ Perform a security assessment to detect security vulnerabilities.

Question 87

An information security program should focus on:

- ☐ best practices also in place at peer companies.
- ☐ solutions codified in international standards.
- ☐ key controls identified in risk assessments.
- ☐ continued process improvement.

Question 88

Security risk assessments should cover only information assets that:

- ☐ are classified and labeled.
- ☐ are inside the organization.
- ☐ support business processes.
- ☐ have tangible value.

Question 89

Which of the following is the MOST effective type of access control?

- ☐ Centralized
- ☐ Role-based
- ☐ Decentralized
- ☐ Discretionary

Question 90

Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

- ☐ Filter media access control (MAC) addresses
- ☐ Use a Wi-Fi Protected Access (WPA2) protocol
- ☐ Use a Wired Equivalent Privacy (WEP) key
- ☐ Web-based authentication

Question 91

Recovery point objectives (RPOs) can be used to determine which of the following?

- ☐ Maximum tolerable period of data loss
- ☐ Maximum tolerable downtime
- ☐ Baseline for operational resiliency
- ☐ Time to restore backups

Question 92

Who can BEST advocate the development of and ensure the success of an information security program?

- ☐ Internal auditor
- ☐ Chief operating officer (COO)
- ☐ Steering committee
- ☐ IT management

Question 93

An information security manager has been asked to develop a change control process. What is the FIRST thing the information security manager should do?

- ☐ Research best practices
- ☐ Meet with stakeholders
- ☐ Establish change control procedures
- ☐ Identify critical systems

Question 94

One way to determine control effectiveness is by determining:

- ☐ whether it is preventive, detective or compensatory.
- ☐ the capability of providing notification of failure.
- ☐ the test results of intended objectives.
- ☐ the evaluation and analysis of reliability.

Question 95

Deciding the level of protection a particular asset should be given in BEST determined by:

- ☐ a threat assessment.
- ☐ a vulnerability assessment.
- ☐ a risk analysis.
- ☐ corporate risk appetite.

Question 96

Executive leadership has decided to engage a consulting firm to develop and implement a comprehensive security framework for the organization to allow senior management to remain focused on business priorities. Which of the following poses the GREATEST challenge to the successful implementation of a new security governance framework?

- ☐ Information security management does not fully accept the responsibility for information security governance.
- ☐ Executive leadership views information security governance primarily as a concern of the information security management team.
- ☐ Information security staff has little or no experience with the practice of information security governance.
- ☐ Executive leadership becomes involved in decisions about information security governance.

Question 97

Which of the following MOST efficiently ensures the proper installation of a firewall policy that restricts a small group of internal IP addresses from accessing the Internet?

- ☐ A connectivity test from the restricted host
- ☐ A simulated denial of service attack against the firewall
- ☐ A port scan of the firewall from an external source
- ☐ A review of the current firewall configuration

Question 98

The business continuity policy should contain which of the following?

- ☐ Emergency call trees
- ☐ Recovery criteria
- ☐ Business impact assessment (BIA)
- ☐ Critical backups inventory

Question 99

Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

- ☐ Security compliant servers trend report
- ☐ Percentage of security compliant servers
- ☐ Number of security patches applied
- ☐ Security patches applied trend report

Question 100

Which of the following is the MOST effective method to prevent an SQL injection in an employee portal?

- ☐ Reconfigure the database schema
- ☐ Enforce referential integrity on the database
- ☐ Conduct code reviews
- ☐ Conduct network penetration testing

Question 101

To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

- ☐ review the functionalities and implementation requirements of the solution.
- ☐ review comparison reports of tool implementation in peer companies.
- ☐ provide examples of situations where such a tool would be useful.
- ☐ substantiate the investment in meeting organizational needs.

Question 102

During an incident, which of the following entities would MOST likely be contacted directly by an organization's incident response team without management approval?

- ☐ Industry regulators
- ☐ Technology vendor
- ☐ Law enforcement
- ☐ Internal audit

Question 103

An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organization's information security manager?

- ☐ The change did not include a proper assessment of risk.
- ☐ Documentation of the change was made after implementation.
- ☐ The information security manager did not review the change prior to implementation.
- ☐ The operations team implemented the change without regression testing.

Question 104

Information classification is a fundamental step in determining:

- ☐ whether risk analysis objectives are met.
- ☐ who has ownership of information.
- ☐ the type of metrics that should be captured.
- ☐ the security strategy that should be used.

Question 105

Who in an organization has the responsibility for classifying information?

- ☐ Data custodian
- ☐ Database administrator
- ☐ Information security officer
- ☐ Data owner

Question 106

Which of the following devices, when placed in a demilitarized zone (DMZ), would be considered the MOST significant exposure?

- ☐ Proxy server
- ☐ Mail relay server
- ☐ Application server
- ☐ Database server

Question 107

A border router should be placed on which of the following?

- ☐ Web server
- ☐ IDS server
- ☐ Screened subnet
- ☐ Domain boundary

Question 108

When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSL), confidentiality is MOST vulnerable to which of the following?

- ☐ IP spoofing
- ☐ Man-in-the-middle attack
- ☐ Repudiation
- ☐ Trojan

Question 109

When performing an information risk analysis, an information security manager should FIRST:

- ☐ establish the ownership of assets.
- ☐ evaluate the risks to the assets.
- ☐ take an asset inventory.
- ☐ categorize the assets.

Question 110

What would be the PRIMARY reason for an organization to conduct a simulated phishing attack on its employees as part of a social engineering assessment?

- ☐ Measure the effectiveness of security awareness training.
- ☐ Identify the need for mitigating security controls.
- ☐ Measure the effectiveness of the anti-spam solution.
- ☐ Test the effectiveness of the incident response plan.

Question 111

What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

- ☐ Functional requirements are not adequately considered.
- ☐ User training programs may be inadequate.
- ☐ Budgets allocated to business units are not appropriate.
- ☐ Information security plans are not aligned with business requirements

Question 112

Which of the following would be the BEST metric for the IT risk management process?

- ☐ Number of risk management action plans
- ☐ Percentage of critical assets with budgeted remedial
- ☐ Percentage of unresolved risk exposures
- ☐ Number of security incidents identified

Question 113

Which would be the BEST recommendation to protect against phishing attacks?

- ☐ Install an antispam system
- ☐ Publish security guidance for customers
- ☐ Provide security awareness to the organization's staff
- ☐ Install an application-level firewall

Question 114

During the security review of organizational servers, it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs. As a FIRST step, the security manager should:

- ☐ copy sample files as evidence.
- ☐ remove access privileges to the folder containing the data.
- ☐ report this situation to the data owner.
- ☐ train the HR team on properly controlling file permissions.

Question 115

The BEST way to identify the criticality of systems to the business is through:

- ☐ a threat assessment.
- ☐ an asset classification.
- ☐ a vulnerability assessment.
- ☐ an impact assessment.

Question 116

Which of the following is a benefit of information security governance?

- ☐ Reduction of the potential for civil or legal liability
- ☐ Questioning trust in vendor relationships
- ☐ Increasing the risk of decisions based on incomplete management information
- ☐ Direct involvement of senior management in developing control processes

Question 117

A semi-annual disaster recovery test has been completed. Which of the following issues discussed during the lessons learned phase should be of GREATEST concern?

- ☐ A server used in recovery did not have the latest security patches
- ☐ Application testing was completed by system administrators
- ☐ Poor network performance was reported during recovery
- ☐ Some restored systems were not listed in the DNS table of the DR subnet

Question 118

When an emergency security patch is received via electronic mail, the patch should FIRST be:

- ☐ loaded onto an isolated test machine.
- ☐ decompiled to check for malicious code.
- ☐ validated to ensure its authenticity.
- ☐ copied onto write-once media to prevent tampering.

Question 119

A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

- ☐ Risk analysis results
- ☐ Audit report findings
- ☐ Penetration test results
- ☐ Amount of IT budget available

Question 120

What is the BEST method to verify that all security patches applied to servers were properly documented?

- ☐ Trace change control requests to operating system (OS) patch logs
- ☐ Trace OS patch logs to OS vendor's update documentation
- ☐ Trace OS patch logs to change control requests
- ☐ Review change control documentation for key servers

Question 121

An unauthorized user gained access to a merchant's database server and customer credit card information. Which of the following would be the FIRST step to preserve and protect unauthorized intrusion activities?

- ☐ Shut down and power off the server.
- ☐ Duplicate the hard disk of the server immediately.
- ☐ Isolate the server from the network.
- ☐ Copy the database log file to a protected server.

Question 122

Which of the following will BEST prevent external security attacks?

- ☐ Static IP addressing
- ☐ Network address translation
- ☐ Background checks for temporary employees
- ☐ Securing and analyzing system access logs

Question 123

A company's mail server allows anonymous file transfer protocol (FTP) access which could be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

- ☐ A penetration test
- ☐ A security baseline review
- ☐ A risk assessment
- ☐ A business impact analysis (BIA)

Question 124

Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

- ☐ Vulnerability scans
- ☐ Penetration tests
- ☐ Code reviews
- ☐ Security audits

Question 125

The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

- ☐ messages displayed at every logon.
- ☐ periodic security-related e-mail messages.
- ☐ an Intranet web site for information security.
- ☐ circulating the information security policy.

Question 126

Which of the following is the MOST effective way to detect information security incidents?

- ☐ Providing regular and up-to-date training for the incident response team
- ☐ Establishing proper policies for response to threats and vulnerabilities
- ☐ Performing regular testing of the incident response program
- ☐ Educating and users on threat awareness and timely reporting

Question 127

Who should be responsible for enforcing access rights to application data?

- ☐ Data owners
- ☐ Business process owners
- ☐ The security steering committee
- ☐ Security administrators

Question 128

Following a significant change to the underlying code of an application, it is MOST important for the information security manager to:

- ☐ inform senior management
- ☐ update the risk assessment
- ☐ validate the user acceptance testing
- ☐ modify key risk indicators

Question 129

An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

- ☐ bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
- ☐ establish baseline standards for all locations and add supplemental standards as required.
- ☐ bring all locations into conformity with a generally accepted set of industry best practices.
- ☐ establish a baseline standard incorporating those requirements that all jurisdictions have in common.

Question 130

A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

- ☐ Prevent the system from being accessed remotely
- ☐ Create a strong random password
- ☐ Ask for a vendor patch
- ☐ Track usage of the account by audit trails

Question 131

Which of the following would provide the MOST effective security outcome in an organization's contract management process?

- ☐ Extending security assessment to include random penetration testing
- ☐ Extending security assessment to cover asset disposal on contract termination
- ☐ Performing vendor security benchmark analyses at the request-for-proposal stage
- ☐ Ensuring security requirements are defined at the request-for-proposal stage

Question 132

An incident response policy must contain:

- ☐ updated call trees.
- ☐ escalation criteria.
- ☐ press release templates.
- ☐ critical backup files inventory.

Question 133

Which of the following change management procedures is MOST likely to cause concern to the information security manager?

- ☐ Fallback processes are tested the weekend before changes are made.
- ☐ The development manager migrates programs into production.
- ☐ A manual rather than an automated process is used to compare program versions.
- ☐ Users are not notified of scheduled system changes.

Question 134

Which of the following is the BEST way to identify the potential impact of a successful attack on an organization's mission critical applications?

- ☐ Conduct penetration testing.
- ☐ Execute regular vulnerability scans.
- ☐ Perform independent code review.
- ☐ Perform application vulnerability review.

Question 135

A validated patch to address a new vulnerability that may affect a mission-critical server has been released. What should be done immediately?

- ☐ Add mitigating controls.
- ☐ Take the server off-line and install the patch.
- ☐ Check the server's security and install the patch.
- ☐ Conduct an impact analysis.

Question 136

Which of the following steps in conducting a risk assessment should be performed FIRST?

- ☐ Identity business assets
- ☐ Identify business risks
- ☐ Assess vulnerabilities
- ☐ Evaluate key controls

Question 137

Which of the following is the BEST way for an organization to ensure that incident response teams are properly prepared?

- ☐ Conducting tabletop exercises appropriate for the organization
- ☐ Providing training from third-party forensics firms
- ☐ Documenting multiple scenarios for the organization and response steps
- ☐ Obtaining industry certifications for the response team

Question 138

Senior management asks the information security manager for justification before approving the acquisition of a new intrusion detection system (IDS). The BEST course of action is to provide:

- ☐ documented industry best practices
- ☐ a gap analysis against the new IDS controls.
- ☐ a business case.
- ☐ a business impact analysis (BIA).

Question 139

In an organization, information systems security is the responsibility of:

- ☐ all personnel.
- ☐ information systems personnel.
- ☐ information systems security personnel.
- ☐ functional personnel.

Question 140

All risk management activities are PRIMARILY designed to reduce impacts to:

- ☐ a level defined by the security manager.
- ☐ an acceptable level based on organizational risk tolerance.
- ☐ a minimum level consistent with regulatory requirements.
- ☐ the minimum level possible.

Question 141

The MOST important reason that statistical anomaly-based intrusion detection systems (stat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

- ☐ create more overhead than signature-based IDSs.
- ☐ cause false positives from minor changes to system variables.
- ☐ generate false alarms from varying user or system actions.
- ☐ cannot detect new types of attacks.

Question 142

Good information security standards should:

- ☐ define precise and unambiguous allowable limits.
- ☐ describe the process for communicating violations.
- ☐ address high-level objectives of the organization.
- ☐ be updated frequently as new software is released.

Question 143

When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

- ☐ services delivery objective.
- ☐ recovery time objective (RTO).
- ☐ recovery window.
- ☐ maximum tolerable outage (MTO).

Question 144

Which of the following is the MOST important element to ensure the successful recovery of a business during a disaster?

- ☐ Detailed technical recovery plans are maintained offsite
- ☐ Network redundancy is maintained through separate providers
- ☐ Hot site equipment needs are recertified on a regular basis
- ☐ Appropriate declaration criteria have been established

Question 145

An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is MOST important to:

- ☐ prohibit remote access to the site.
- ☐ periodically recertify access rights.
- ☐ enforce document lifecycle management.
- ☐ conduct a vulnerability assessment.

Question 146

Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

- ☐ Tuning
- ☐ Patching
- ☐ Encryption
- ☐ Packet filtering

Question 147

The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

- ☐ enable independent and objective review of the root cause of the incidents.
- ☐ obtain support for enhancing the expertise of the third-party teams.
- ☐ identify lessons learned for further improving the information security management process.
- ☐ obtain better buy-in for the information security program.

Question 148

Which of the following devices should be placed within a DMZ?

- ☐ Proxy server
- ☐ Application server
- ☐ Departmental server
- ☐ Data warehouse server

Question 149

Which of the following BEST demonstrates alignment between information security governance and corporate governance?

- ☐ Average number of security incidents across business units
- ☐ Security project justifications provided in terms of business value
- ☐ Number of vulnerabilities identified for high-risk information assets
- ☐ Mean time to resolution for enterprise-wide security incidents

Question 150

The PRIMARY focus of the change control process is to ensure that changes are:

- ☐ authorized.
- ☐ applied.
- ☐ documented.
- ☐ tested.

Question 151

Information security policies should:

- ☐ address corporate network vulnerabilities.
- ☐ address the process for communicating a violation.
- ☐ be straightforward and easy to understand.
- ☐ be customized to specific groups and roles.

Question 152

An organization without any formal information security program that has decided to implement information security best practices should FIRST:

- ☐ invite an external consultant to create the security strategy.
- ☐ allocate budget based on best practices.
- ☐ benchmark similar organizations.
- ☐ define high-level business security requirements.

Question 153

Which of the following should be the PRIMARY focus of a post-incident review following a successful response to a cybersecurity incident?

- ☐ Which control failures contributed to the incident
- ☐ How incident response processes were executed
- ☐ What attack vectors were utilized
- ☐ When business operations were restored

Question 154

Which of the following will BEST protect against malicious activity by a former employee?

- ☐ Preemployment screening
- ☐ Close monitoring of users
- ☐ Periodic awareness training
- ☐ Effective termination procedures

Question 155

Which of the following roles is PRIMARILY responsible for determining the information classification levels for a given information asset?

- ☐ Manager
- ☐ Custodian
- ☐ User
- ☐ Owner

Question 156

A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

- ☐ rebuild the server from the last verified backup.
- ☐ place the web server in quarantine.
- ☐ shut down the server in an organized manner.
- ☐ rebuild the server with original media and relevant patches.

Question 157

Which of the following BEST illustrates residual risk within an organization?

- ☐ Risk management framework
- ☐ Risk register
- ☐ Business impact analysis
- ☐ Heat map

Question 158

Risk acceptance is a component of which of the following?

- ☐ Assessment
- ☐ Mitigation
- ☐ Evaluation
- ☐ Monitoring

Question 159

Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

- ☐ A hot site facility will be shared in multiple disaster declarations
- ☐ All equipment is provided "at time of disaster, not on floor"
- ☐ The facility is subject to a "first-come, first-served" policy
- ☐ Equipment may be substituted with equivalent model

Question 160

Which of the following is the BEST approach for improving information security management processes?

- ☐ Conduct periodic security audits.
- ☐ Perform periodic penetration testing.
- ☐ Define and monitor security metrics.
- ☐ Survey business units for feedback.

Question 161

Which of the following is the BEST method to protect consumer private information for an online public website?

- ☐ Encrypt consumer's data in transit and at rest.
- ☐ Apply a masking policy to the consumer data.
- ☐ Use secure encrypted transport layer.
- ☐ Apply strong authentication to online accounts.

Question 162

What is the BEST method for mitigating against network denial of service (DoS) attacks?

- ☐ Ensure all servers are up-to-date on OS patches
- ☐ Employ packet filtering to drop suspect packets
- ☐ Implement network address translation to make internal addresses nonroutable
- ☐ Implement load balancing for Internet facing devices

Question 163

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- ☐ Optimized
- ☐ Managed
- ☐ Defined
- ☐ Repeatable

Question 164

Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

- ☐ The information security department has difficulty filling vacancies.
- ☐ The chief information officer (CIO) approves security policy changes.
- ☐ The information security oversight committee only meets quarterly.
- ☐ The data center manager has final signoff on all security projects.

Question 165

The PRIMARY objective of a risk management program is to:

- ☐ minimize inherent risk.
- ☐ eliminate business risk.
- ☐ implement effective controls.
- ☐ minimize residual risk.

Question 166

A multinational organization wants to monitor outbound traffic for data leakage from the use of unapproved cloud services. Which of the following should be the information security manager's GREATEST consideration when implementing this control?

- ☐ Security of cloud services
- ☐ Data privacy regulations
- ☐ Resistance from business users
- ☐ Allocation of monitoring resources

Question 167

A regulatory organization sends an email to an information security manager warning of an impending cyber-attack. The information security manager should FIRST:

- ☐ validate the authenticity of the alert
- ☐ determine whether the attack is in progress
- ☐ alert the network operations center
- ☐ reply asking for more details

Question 168

Why is "slack space" of value to an information security manager as part of an incident investigation?

- ☐ Hidden data may be stored there
- ☐ The slack space contains login information
- ☐ Slack space is encrypted
- ☐ It provides flexible space for the investigation

Question 169

A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

- ☐ Ensure that all OS patches are up-to-date
- ☐ Block inbound traffic until a suitable solution is found
- ☐ Obtain guidance from the firewall manufacturer
- ☐ Commission a penetration test

Question 170

Management decisions concerning information security investments will be MOST effective when they are based on:

- ☐ an annual loss expectancy (ALE) determined from the history of security events.
- ☐ the formalized acceptance of risk analysis by management.
- ☐ the reporting of consistent and periodic assessments of risks.
- ☐ a process for identifying and analyzing threats and vulnerabilities.

Question 171

Which of the following should be the PRIMARY consideration when selecting a recovery site?

- ☐ Regulatory requirements
- ☐ Recovery time objective
- ☐ Geographical location
- ☐ Recovery point objective

Question 172

An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

- ☐ use the test equipment in the warm site facility to read the tapes.
- ☐ retrieve the tapes from the warm site and test them.
- ☐ have duplicate equipment available at the warm site.
- ☐ inspect the facility and inventory the tapes on a quarterly basis.

Question 173

The FIRST step to create an internal culture that focuses on information security is to:

- ☐ implement stronger controls.
- ☐ conduct periodic awareness training.
- ☐ actively monitor operations.
- ☐ gain the endorsement of executive management.

Question 174

An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

- ☐ performance measurement.
- ☐ integration.
- ☐ alignment.
- ☐ value delivery.

Question 175

Which of the following characteristics is MOST important when looking at prospective candidates for the role of chief information security officer (CISO)?

- ☐ Knowledge of information technology platforms, networks and development methodologies
- ☐ Ability to understand and map organizational needs to security technologies
- ☐ Knowledge of the regulatory environment and project management techniques
- ☐ Ability to manage a diverse group of individuals and resources across an organization

Question 176

In risk assessment, after the identification of threats to organizational assets, the information security manager would:

- ☐ evaluate the controls currently in place.
- ☐ implement controls to achieve target risk levels.
- ☐ request funding for the security program.
- ☐ determine threats to be reported to upper management.

Question 177

The FIRST step in establishing a security governance program is to:

- ☐ conduct a risk assessment.
- ☐ conduct a workshop for all end users.
- ☐ prepare a security budget.
- ☐ obtain high-level sponsorship.

Question 178

From an information security perspective, information that no longer supports the main purpose of the business should be:

- ☐ analyzed under the retention policy.
- ☐ protected under the information classification policy.
- ☐ analyzed under the backup policy.
- ☐ protected under the business impact analysis (BIA).

Question 179

Which of the following is MOST likely to be included in an enterprise information security policy?

- ☐ Security monitoring strategy
- ☐ Audit trail review requirements
- ☐ Password composition requirements
- ☐ Consequences of noncompliance

Question 180

Which of the following is MOST difficult to achieve in a public cloud-computing environment?

- ☐ Cost reduction
- ☐ Pay per use
- ☐ On-demand provisioning
- ☐ Ability to audit

Question 181

Which of the following will MOST likely reduce the chances of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have his, her password reset?

- ☐ Performing reviews of password resets
- ☐ Conducting security awareness programs
- ☐ Increasing the frequency of password changes
- ☐ Implementing automatic password syntax checking

Question 182

The MOST likely cause of a security information event monitoring (SIEM) solution failing to identify a serious incident is that the system:

- ☐ is not collecting logs from relevant devices.
- ☐ has not been updated with the latest patches.
- ☐ is hosted by a cloud service provider.
- ☐ has performance issues.

Question 183

Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

- ☐ Business continuity coordinator
- ☐ Chief operations officer (COO)
- ☐ Information security manager
- ☐ Internal audit

Question 184

Prior to having a third party perform an attack and penetration test against an organization, the MOST important action is to ensure that:

- ☐ the third party provides a demonstration on a test system.
- ☐ goals and objectives are clearly defined.
- ☐ the technical staff has been briefed on what to expect.
- ☐ special backups of production servers are taken.

Question 185

When implementing a new risk assessment methodology, which of the following is the MOST important requirement?

- ☐ Risk assessments must be conducted by certified staff.
- ☐ The methodology must be approved by the chief executive officer.
- ☐ Risk assessments must be reviewed annually.
- ☐ The methodology used must be consistent across the organization.

Question 186

Which of the following is the BEST reason for reevaluating an information security program?

- ☐ Ineffectiveness of the information security strategy execution
- ☐ Misalignment between information security priorities and business objectives
- ☐ Change in senior management
- ☐ Noncompliance with information security policies and procedures

Question 187

An organization is considering whether to allow employees to use personal computing devices for business purposes. To BEST facilitate senior management's decision, the information security manager should:

- ☐ map the strategy to business objectives
- ☐ perform a cost-benefit analysis
- ☐ conduct a risk assessment
- ☐ develop a business case

Question 188

Which of the following is a PRIMARY responsibility of an information security governance committee?

- ☐ Analyzing information security policy compliance reviews
- ☐ Approving the purchase of information security technologies
- ☐ Reviewing the information security strategy
- ☐ Approving the information security awareness training strategy

Question 189

Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

- ☐ The security officer
- ☐ Senior management
- ☐ The end user
- ☐ The custodian

Question 190

Detailed business continuity plans should be based PRIMARILY on:

- ☐ consideration of different alternatives.
- ☐ the solution that is least expensive.
- ☐ strategies that cover all applications.
- ☐ strategies validated by senior management.

Question 191

Which of the following is the PRIMARY goal of a risk management program?

- ☐ Implement preventive controls against threats.
- ☐ Manage the business impact of inherent risks.
- ☐ Manage compliance with organizational policies.
- ☐ Reduce the organization's risk appetite.

Question 192

Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

- ☐ Security policies and procedures
- ☐ Annual self-assessment by management
- ☐ Security-steering committees
- ☐ Security awareness campaigns

Question 193

Which of the following is the PRIMARY reason for performing an analysis of the threat landscape on a regular basis?

- ☐ To determine the basis for proposing an increase in security budgets.
- ☐ To determine if existing business continuity plans are adequate.
- ☐ To determine if existing vulnerabilities present a risk.
- ☐ To determine critical information for executive management.

Question 194

The PRIMARY purpose of aligning information security with corporate governance objectives is to:

- ☐ build capabilities to improve security processes.
- ☐ consistently manage significant areas of risk.
- ☐ identify an organization's tolerance for risk.
- ☐ re-align roles and responsibilities.

Question 195

There is reason to believe that a recently modified web application has allowed unauthorized access. Which is the BEST way to identify an application backdoor?

- ☐ Black box pen test
- ☐ Security audit
- ☐ Source code review
- ☐ Vulnerability scan

Question 196

An organization has detected potential risk emerging from noncompliance with new regulations in its industry.

Which of the following is the MOST important reason to report this situation to senior management?

- ☐ The risk profile needs to be updated.
- ☐ An external review of the risk needs to be conducted.
- ☐ Specific monitoring controls need to be implemented.
- ☐ A benchmark analysis needs to be performed.

Question 197

The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

- ☐ head of internal audit.
- ☐ chief operations officer (COO).
- ☐ chief technology officer (CTO).
- ☐ legal counsel.

Question 198

An organization has implemented an enhanced password policy for business applications which requires significantly more business unit resource to support clients. The BEST approach to obtain the support of business unit management would be to:

- ☐ present an analysis of the cost and benefit of the changes
- ☐ discuss the risk and impact of security incidents if not implemented
- ☐ present industry benchmarking results to business units
- ☐ elaborate on the positive impact to information security

Question 199

Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

- ☐ Screened subnets
- ☐ Information classification policies and procedures
- ☐ Role-based access controls
- ☐ Intrusion detection system (IDS)

Question 200

The purpose of a corrective control is to:

- ☐ reduce adverse events.
- ☐ indicate compromise.
- ☐ mitigate impact.
- ☐ ensure compliance.

Question 201

To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

- ☐ revise the information security program.
- ☐ evaluate a balanced business scorecard.
- ☐ conduct regular user awareness sessions.
- ☐ perform penetration tests.

Question 202

Retention of business records should PRIMARILY be based on:

- ☐ business strategy and direction.
- ☐ regulatory and legal requirements.
- ☐ storage capacity and longevity.
- ☐ business ease and value analysis.

Question 203

Which of the following is the MOST important step in risk ranking?

- ☐ Impact assessment
- ☐ Mitigation cost
- ☐ Threat assessment
- ☐ Vulnerability analysis

Question 204

An information security manager learns that the root password of an external FTP server may be subject to brute force attacks. Which of the following would be the MOST appropriate way to reduce the likelihood of a successful attack?

- ☐ Block the source IP address of the attacker.
- ☐ Lock remote logon after multiple failed attempts.
- ☐ Disable access to the externally facing server.
- ☐ Install an intrusion detection system (IDS).

Question 205

What is the PRIMARY role of the information security manager in the process of information classification within an organization?

- ☐ Defining and ratifying the classification structure of information assets
- ☐ Deciding the classification levels applied to the organization's information assets
- ☐ Securing information assets in accordance with their classification
- ☐ Checking if information assets have been classified properly

Question 206

The effectiveness of virus detection software is MOST dependent on which of the following?

- ☐ Packet filtering
- ☐ Intrusion detection
- ☐ Software upgrades
- ☐ Definition tables

Question 207

An organization outsources its payroll processing. Which of the following would be the BEST key risk indicator for monitoring the information security of the service provider?

- ☐ Number of security incidents by severity
- ☐ Number of critical security patches
- ☐ Percentage of application up-time
- ☐ Number of manual payroll adjustments

Question 208

Which of the following is the MOST significant security risk in IT asset management?

- ☐ IT assets may be used by staff for private purposes
- ☐ Unregistered IT assets may not be supported
- ☐ Unregistered IT assets may not be included in security documentation
- ☐ Unregistered IT assets may not be configured properly

Question 209

Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

- ☐ An intrusion prevention system (IPS)
- ☐ An intrusion detection system (IDS)
- ☐ A host-based intrusion detection system (HIDS)
- ☐ A host-based firewall

Question 210

Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

- ☐ Patch management
- ☐ Change management
- ☐ Security baselines
- ☐ Acquisition management

Question 211

The BEST way to justify the implementation of a single sign-on (SSO) product is to use:

- ☐ return on investment (ROI).
- ☐ a vulnerability assessment.
- ☐ annual loss expectancy (ALE).
- ☐ a business case.

Question 212

The information classification scheme should:

- ☐ consider possible impact of a security breach.
- ☐ classify personal information in electronic form.
- ☐ be performed by the information security manager.
- ☐ classify systems according to the data processed.

Question 213

Which of the following devices should be placed within a demilitarized zone (DMZ)?

- ☐ Network switch
- ☐ Web server
- ☐ Database server
- ☐ File/print server

Question 214

An information security manager has been asked to create a strategy to protect the organization's information from a variety of threat vectors. Which of the following should be done FIRST?

- ☐ Perform a threat modeling exercise
- ☐ Develop a risk profile
- ☐ Design risk management processes
- ☐ Select a governance framework

Question 215

Which of the following events generally has the highest information security impact?

- ☐ Opening a new office
- ☐ Merging with another organization
- ☐ Relocating the data center
- ☐ Rewiring the network

Question 216

An intrusion detection system (IDS) should:

- ☐ run continuously
- ☐ ignore anomalies
- ☐ require a stable, rarely changed environment
- ☐ be located on the network

Question 217

When messages are encrypted and digitally signed to protect documents transferred between trading partners, the GREATEST concern is that:

- ☐ trading partners can repudiate the transmission of messages.
- ☐ hackers can eavesdrop on messages.
- ☐ trading partners can repudiate the receipt of messages.
- ☐ hackers can introduce forgery messages.

Question 218

What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

- ☐ all use weak encryption.
- ☐ are decrypted by the firewall.
- ☐ may be quarantined by mail filters.
- ☐ may be corrupted by the receiving mail server.

Question 219

Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

- ☐ Security audit reports
- ☐ Balanced scorecard
- ☐ Capability maturity model (CMM)
- ☐ Systems and business security architecture

Question 220

The PRIMARY reason for establishing a data classification scheme is to identify:

- ☐ data ownership.
- ☐ data-retention strategy.
- ☐ appropriate controls.
- ☐ recovery priorities.

Question 221

Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

- ☐ System analyst
- ☐ System user
- ☐ Operations manager
- ☐ Data security officer

Question 222

Which of the following would BEST provide stakeholders with information to determine the appropriate response to a disaster?

- ☐ Risk assessment
- ☐ Vulnerability assessment
- ☐ Business impact analysis
- ☐ SWOT analysis

Question 223

The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

- ☐ IT assets in key business functions are protected.
- ☐ business risks are addressed by preventive controls.
- ☐ stated objectives are achievable.
- ☐ IT facilities and systems are always available.

Question 224

Which of the following is MOST appropriate for inclusion in an information security strategy?

- ☐ Business controls designated as key controls
- ☐ Security processes, methods, tools and techniques
- ☐ Firewall rule sets, network defaults and intrusion detection system (IDS) settings
- ☐ Budget estimates to acquire specific security tools

Question 225

Which of the following should be the PRIMARY basis for an information security strategy?

- ☐ The organization's vision and mission.
- ☐ Information security policies.
- ☐ Results of a comprehensive gap analysis.
- ☐ Audit and regulatory requirements.

Question 226

An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

- ☐ corporate data privacy policy.
- ☐ data privacy policy where data are collected.
- ☐ data privacy policy of the headquarters' country.
- ☐ data privacy directive applicable globally.

Question 227

Which of the following is a key area of the ISO 27001 framework?

- ☐ Operational risk assessment
- ☐ Financial crime metrics
- ☐ Capacity management
- ☐ Business continuity management

Question 228

The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

- ☐ service level monitoring.
- ☐ penetration testing.
- ☐ periodically auditing.
- ☐ security awareness training.

Question 229

A computer incident response team (CIRT) manual should PRIMARILY contain which of the following documents?

- ☐ Risk assessment results
- ☐ Severity criteria
- ☐ Emergency call tree directory
- ☐ Table of critical backup files

Question 230

Acceptable levels of information security risk should be determined by:

- ☐ legal counsel.
- ☐ security management.
- ☐ external auditors.
- ☐ die steering committee.

Question 231

Which of the following measures is the MOST effective deterrent against disgruntled staff abusing their privileges?

- ☐ Layered defense strategy
- ☐ System audit log monitoring
- ☐ Signed acceptable use policy
- ☐ High-availability systems

Question 232

Which of the following metrics would be the MOST useful in measuring how well information security is monitoring violation logs?

- ☐ Penetration attempts investigated
- ☐ Violation log reports produced
- ☐ Violation log entries
- ☐ Frequency of corrective actions taken

Question 233

The PRIMARY goal of a post-incident review should be to:

- ☐ determine why the incident occurred.
- ☐ determine how to improve the incident handling process.
- ☐ identify policy changes to prevent a recurrence.
- ☐ establish the cost of the incident to the business.

Question 234

Which of the following would be MOST helpful in determining an organization's current capacity to mitigate risk?

- ☐ Capability maturity model
- ☐ Business impact analysis
- ☐ IT security risk and exposure
- ☐ Vulnerability assessment

Question 235

Management has announced the acquisition of a new company. The information security manager of parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies.

To BEST address this concern, the information security manager should:

- ☐ escalate concern for conflicting access rights to management.
- ☐ implement consistent access control standards.
- ☐ review access rights as the acquisition integration occurs.
- ☐ perform a risk assessment of the access rights.

Question 236

Previously accepted risk should be:

- ☐ re-assessed periodically since the risk can be escalated to an unacceptable level due to revised conditions.
- ☐ accepted permanently since management has already spent resources (time and labor) to conclude that the risk level is acceptable.
- ☐ avoided next time since risk avoidance provides the best protection to the company.
- ☐ removed from the risk log once it is accepted.

Question 237

An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

- ☐ Security metrics reports
- ☐ Risk assessment reports
- ☐ Business impact analysis (BIA)
- ☐ Return on security investment report

Question 238

Which of the following would represent a violation of the chain of custody when a backup tape has been identified as evidence in a fraud investigation? The tape was:

- ☐ removed into the custody of law enforcement investigators.
- ☐ kept in the tape library' pending further analysis.
- ☐ sealed in a signed envelope and locked in a safe under dual control.
- ☐ handed over to authorized independent investigators.

Question 239

Which of the following is the BEST way to align security and business strategies?

- ☐ Include security risk as part of corporate risk management.
- ☐ Develop a balanced scorecard for security.
- ☐ Establish key performance indicators (KPIs) for business through security processes.
- ☐ Integrate information security governance into corporate governance.

Question 240

When outsourcing information security administration, it is MOST important for an organization to include:

- ☐ nondisclosure agreements (NDAs)
- ☐ contingency plans
- ☐ insurance requirements
- ☐ service level agreements (SLAs)

Question 241

Which of the following actions should be taken when an information security manager discovers that a hacker is foot printing the network perimeter?

- ☐ Reboot the border router connected to the firewall
- ☐ Check IDS logs and monitor for any active attacks
- ☐ Update IDS software to the latest available version
- ☐ Enable server trace logging on the DMZ segment

Question 242

Which of the following is the MOST effective approach for delivering security incident response training?

- ☐ Perform role-playing exercises to simulate real-world incident response scenarios.
- ☐ Engage external consultants to present real-world examples within the industry.
- ☐ Include incident response training within new staff orientation.
- ☐ Provide on-the-job training and mentoring for the incident response team.

Question 243

Which of the following will BEST protect confidential data when connecting large wireless networks to an existing wired-network infrastructure?

- ☐ Mandatory access control (MAC) address filtering
- ☐ Strong passwords
- ☐ Virtual private network (VPN)
- ☐ Firewall

Question 244

An organization has determined that one of its web servers has been compromised. Which of the following actions should be taken to preserve the evidence of the intrusion for forensic analysis and potential litigation?

- ☐ Reboot the server in a secure area to search for digital evidence.
- ☐ Unplug the server from the power.
- ☐ Restrict physical and logical access to the server.
- ☐ Run analysis tools to detect the source of the intrusion.

Question 245

An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's FIRST step to support this strategy?

- ☐ Incorporate social media into the security awareness program.
- ☐ Develop a guideline on the acceptable use of social media.
- ☐ Develop a business case for a data loss prevention solution.
- ☐ Employ the use of a web content filtering solution.

Question 246

Which of the following is the MOST important element of an information security strategy?

- ☐ Defined objectives
- ☐ Time frames for delivery
- ☐ Adoption of a control framework
- ☐ Complete policies

Question 247

An organization performed a risk analysis and found a large number of assets with low-impact vulnerabilities. The NEXT action of the information security manager should be to:

- ☐ determine appropriate countermeasures.
- ☐ transfer the risk to a third party.
- ☐ report to management.
- ☐ quantify the aggregated risk.

Question 248

The GREATEST benefit resulting from well-documented information security procedures is that they:

- ☐ ensure that security policies are consistently applied.
- ☐ ensure that critical processes can be followed by temporary staff.
- ☐ facilitate security training of new staff.
- ☐ provide a basis for auditing security practices.

Question 249

Which of the following is the MOST important information to include in a strategic plan for information security?

- ☐ Information security staffing requirements
- ☐ Current state and desired future state
- ☐ IT capital investment requirements
- ☐ information security mission statement

Question 250

The PRIMARY disadvantage of using a cold-site recovery facility is that it is:

- ☐ unavailable for testing during normal business hours.
- ☐ only available if not being used by the primary tenant.
- ☐ not possible to reserve test dates in advance.
- ☐ not cost-effective for testing critical applications at the site.

Question 251

Which of the following is MOST important to the successful development of an information security strategy?

- ☐ A well-implemented governance framework
- ☐ Current state and desired objectives
- ☐ An implemented development life cycle process
- ☐ Approved policies and standards

Question 252

Which of the following is a PRIMARY security responsibility of an information owner?

- ☐ Deciding what level of classification the information requires
- ☐ Testing information classification controls
- ☐ Maintaining the integrity of data in the information system
- ☐ Determining the controls associated with information classification

Question 253

If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

- ☐ obtaining evidence as soon as possible.
- ☐ preserving the integrity of the evidence.
- ☐ disconnecting all IT equipment involved.
- ☐ reconstructing the sequence of events.

Question 254

The MOST important reason to have a well-documented and tested incident response plan in place is to:

- ☐ standardize the chain of custody procedure
- ☐ facilitate the escalation process
- ☐ promote a coordinated effort.
- ☐ outline external communications

Question 255

Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

- ☐ Disclosure of personal information
- ☐ Sufficient coverage of the insurance policy for accidental losses
- ☐ Intrinsic value of the data stored on the equipment
- ☐ Replacement cost of the equipment

Question 256

Security audit reviews should PRIMARILY:

- ☐ ensure that controls operate as required.
- ☐ ensure that controls are cost-effective.
- ☐ focus on preventive controls.
- ☐ ensure controls are technologically current.

Question 257

The likelihood of a successful attack is a function of:

- ☐ incentive and capability of the intruder
- ☐ opportunity and asset value
- ☐ threat and vulnerability levels
- ☐ value and desirability to the intruder

Question 258

An information security manager discovers that the organization's new information security policy is not being followed across all departments. Which of the following should be of GREATEST concern to the information security manager?

- ☐ Different communication methods may be required for each business unit.
- ☐ Business unit management has not emphasized the importance of the new policy.
- ☐ The corresponding controls are viewed as prohibitive to business operations.
- ☐ The wording of the policy is not tailored to the audience.

Question 259

An organization has an approved bring your own device (BYOD) program. Which of the following is the MOST effective method to enforce application control on personal devices?

- ☐ Establish a mobile device acceptable use policy.
- ☐ Implement a mobile device management solution.
- ☐ Educate users regarding the use of approved applications.
- ☐ Implement a web application firewall.

Question 260

An information security manager developing an incident response plan MUST ensure it includes:

- ☐ an inventory of critical data
- ☐ criteria for escalation
- ☐ critical infrastructure diagrams
- ☐ a business impact analysis

Question 261

The configuration management plan should PRIMARILY be based upon input from:

- ☐ business process owners.
- ☐ the information security manager.
- ☐ the security steering committee.
- ☐ IT senior management.

Question 262

Which of the following is MOST essential for a risk management program to be effective?

- ☐ Flexible security budget
- ☐ Sound risk baseline
- ☐ New risks detection
- ☐ Accurate risk reporting

Question 263

When supporting an organization's privacy officer, which of the following is the information security manager's PRIMARY role regarding privacy requirements?

- ☐ Monitoring the transfer of private data
- ☐ Conducting privacy awareness programs
- ☐ Ensuring appropriate controls are in place
- ☐ Determining data classification

Question 264

The MOST basic requirement for an information security governance program is to:

- ☐ be aligned with the corporate business strategy.
- ☐ be based on a sound risk management approach.
- ☐ provide adequate regulatory compliance.
- ☐ provide best practices for security- initiatives.

Question 265

When identifying legal and regulatory issues affecting information security, which of the following would represent the BEST approach to developing information security policies?

- ☐ Create separate policies to address each regulation
- ☐ Develop policies that meet all mandated requirements
- ☐ Incorporate policy statements provided by regulators
- ☐ Develop a compliance risk assessment

Question 266

After assessing and mitigating the risks of a web application, who should decide on the acceptance of residual application risks?

- ☐ Information security officer
- ☐ Chief information officer (CIO)
- ☐ Business owner
- ☐ Chief executive officer (CEO)

Question 267

A risk management approach to information protection is:

- ☐ managing risks to an acceptable level, commensurate with goals and objectives.
- ☐ accepting the security posture provided by commercial security products.
- ☐ implementing a training program to educate individuals on information protection and risks.
- ☐ managing risk tools to ensure that they assess all information protection vulnerabilities.

Question 268

Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

- ☐ The number of false positives increases
- ☐ The number of false negatives increases
- ☐ Active probing is missed
- ☐ Attack profiles are ignored

Question 269

When considering whether to adopt a new information security framework, an organization's information security manager should FIRST:

- ☐ compare the framework with the current business strategy
- ☐ perform a technical feasibility analysis
- ☐ perform a financial viability study
- ☐ analyze the framework's legal implications and business impact

Question 270

The contribution of recovery point objective (RPO) to disaster recovery is to:

- ☐ define backup strategy.
- ☐ eliminate single points of failure.
- ☐ reduce mean time between failures (MTBF).
- ☐ minimize outage period.

Question 271

An information security manager is developing a business case for an investment in an information security control. The FIRST step should be to:

- ☐ research vendor pricing to show cost efficiency
- ☐ assess potential impact to the organization
- ☐ demonstrate increased productivity of security staff
- ☐ gain audit buy-in for the security control

Question 272

Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?

- ☐ Communicating specially drafted messages by an authorized person
- ☐ Refusing to comment until recovery
- ☐ Referring the media to the authorities
- ☐ Reporting the losses and recovery strategy to the media

Question 273

Which of the following is the MOST appropriate position to sponsor the design and implementation of a new security infrastructure in a large global enterprise?

- ☐ Chief security officer (CSO)
- ☐ Chief operating officer (COO)
- ☐ Chief privacy officer (CPO)
- ☐ Chief legal counsel (CLC)

Question 274

An information security manager learns that a departmental system is out of compliance with the information security policy's password strength requirements. Which of the following should be the information security manager's FIRST course of action?

- ☐ Submit the issue to the steering committee for escalation
- ☐ Conduct an impact analysis to quantify the associated risk
- ☐ Isolate the non-compliant system from the rest of the network
- ☐ Request risk acceptance from senior management

Question 275

What is the BEST way to ensure that contract programmers comply with organizational security policies?

- ☐ Explicitly refer to contractors in the security standards
- ☐ Have the contractors acknowledge in writing the security policies
- ☐ Create penalties for noncompliance in the contracting agreement
- ☐ Perform periodic security reviews of the contractors

Question 276

What is the MOST important item to be included in an information security policy?

- ☐ The definition of roles and responsibilities
- ☐ The scope of the security program
- ☐ The key objectives of the security program
- ☐ Reference to procedures and standards of the security program

Question 277

A test plan to validate the security controls of a new system should be developed during which phase of the project?

- ☐ Testing
- ☐ Initiation
- ☐ Design
- ☐ Development

Question 278

Which of the following would be MOST helpful to the information security manager tasked with enforcing enhanced password standards?

- ☐ Conducting password strength testing
- ☐ Reeducating end users on creating strong complex passwords
- ☐ Implementing a centralized identity management system
- ☐ Implementing technical password controls to include strong complexity

Question 279

Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

- ☐ Daily
- ☐ Weekly
- ☐ Concurrently with O/S patch updates
- ☐ During scheduled change control updates

Question 280

A data leakage prevention (DLP) solution has identified that several employees are sending confidential company data to their personal email addresses in violation of company policy. The information security manager should FIRST:

- ☐ contact the employees involved to retake security awareness training
- ☐ notify senior management that employees are breaching policy
- ☐ limit access to the Internet for employees involved
- ☐ initiate an investigation to determine the full extent of noncompliance

Question 281

When developing security standards, which of the following would be MOST appropriate to include?

- ☐ Accountability for licenses
- ☐ Acceptable use of IT assets
- ☐ Operating system requirements
- ☐ Inventory management

Question 282

Which of the following authentication methods prevents authentication replay?

- ☐ Password hash implementation
- ☐ Challenge/response mechanism
- ☐ Wired Equivalent Privacy (WEP) encryption usage
- ☐ HTTP Basic Authentication

Question 283

Which of the following is the BEST way to determine if an organization's current risk is within the risk appetite?

- ☐ Conducting a business impact analysis (BIA)
- ☐ Implementing key performance indicators (KPIs)
- ☐ Implementing key risk indicators (KRIs)
- ☐ Developing additional mitigating controls

Question 284

Who should determine data access requirements for an application hosted at an organization's data center?

- ☐ Business owner
- ☐ Information security manager
- ☐ Systems administrator
- ☐ Data custodian

Question 285

Which of the following is the BEST metric for evaluating the effectiveness of security awareness training? The number of:

- ☐ password resets.
- ☐ reported incidents.
- ☐ incidents resolved.
- ☐ access rule violations.

Question 286

Of the following, retention of business records should be PRIMARILY based on:

- ☐ periodic vulnerability assessment.
- ☐ regulatory and legal requirements.
- ☐ device storage capacity and longevity.
- ☐ past litigation.

Question 287

In a cloud technology environment, which of the following would pose the GREATEST challenge to the investigation of security incidents?

- ☐ Access to the hardware
- ☐ Data encryption
- ☐ Non-standard event logs
- ☐ Compressed customer data

Question 288

An organization is in the process of adopting a hybrid data infrastructure, transferring all non-core applications to cloud service providers and maintaining all core business functions house. The information security manager has determined a defense in depth strategy should be used. Which of the following BEST describes this strategy?

- ☐ Multi-factor login requirements for cloud service applications, timeouts, and complex passwords
- ☐ Deployments of nested firewalls within the infrastructure
- ☐ Separate security controls for applications, platforms, programs, and endpoints
- ☐ Strict enforcement of role-based access control (RBAC)

Question 289

Which of the following is the MOST important action when using a web application that has recognized vulnerabilities?

- ☐ Deploy an application firewall.
- ☐ Deploy host-based intrusion detection.
- ☐ Install anti-spyware software.
- ☐ Monitor application level logs.

Question 290

In addition to backup data, which of the following is the MOST important to store offsite in the event of a disaster?

- ☐ Copies of critical contracts and service level agreements (SLAs)
- ☐ Copies of the business continuity plan
- ☐ Key software escrow agreements for the purchased systems
- ☐ List of emergency numbers of service providers

Question 291

When personal information is transmitted across networks, there MUST be adequate controls over:

- ☐ change management.
- ☐ privacy protection.
- ☐ consent to data transfer.
- ☐ encryption devices.

Question 292

Which of the following would help to change an organization's security culture?

- ☐ Develop procedures to enforce the information security policy
- ☐ Obtain strong management support
- ☐ Implement strict technical security controls
- ☐ Periodically audit compliance with the information security policy

Question 293

When defining responsibilities with a cloud computing vendor, which of the following should be regarded as a shared responsibility between user and provider?

- ☐ Data ownership
- ☐ Access log review
- ☐ Application logging
- ☐ Incident response

Question 294

When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

- ☐ Business continuity coordinator
- ☐ Information security manager
- ☐ Business process owners
- ☐ Industry averages benchmarks

Question 295

Which of the following will BEST help to proactively prevent the exploitation of vulnerabilities in operating system software?

- ☐ Patch management
- ☐ Threat management
- ☐ Intrusion detection system
- ☐ Anti-virus software

Question 296

What of the following is MOST important to include in an information security policy?

- ☐ Maturity levels
- ☐ Best practices
- ☐ Management objectives
- ☐ Baselines

Question 297

Security technologies should be selected PRIMARILY on the basis of their:

- ☐ ability to mitigate business risks.
- ☐ evaluations in trade publications.
- ☐ use of new and emerging technologies.
- ☐ benefits in comparison to their costs.

Question 298

To determine the selection of controls required to meet business objectives, an information security manager should:

- ☐ prioritize the use of role-based access controls.
- ☐ focus on key controls.
- ☐ restrict controls to only critical applications.
- ☐ focus on automated controls.

Question 299

Data owners are normally responsible for which of the following?

- ☐ Applying emergency changes to application data
- ☐ Administering security over database records
- ☐ Migrating application code changes to production
- ☐ Determining the level of application security required

Question 300

An intranet server should generally be placed on the:

- ☐ internal network.
- ☐ firewall server.
- ☐ external router.
- ☐ primary domain controller.

Question 301

The PRIMARY objective of performing a post-incident review is to:

- ☐ identify the root cause.
- ☐ identify control improvements.
- ☐ re-evaluate the impact of incidents.
- ☐ identify vulnerabilities.

Question 302

The recovery time objective (RTO) is reached at which of the following milestones?

- ☐ Disaster declaration
- ☐ Recovery of the backups
- ☐ Restoration of the system
- ☐ Return to business as usual processing

Question 303

Which of the following would provide senior management with the BEST information to better understand the organization's information security risk profile?

- ☐ Scenarios that impact business operations
- ☐ Scenarios that disrupt client services
- ☐ Scenarios that impact business goals
- ☐ Scenarios that have a monetary impact

Question 304

Which of the following function is the MOST critical when initiating the removal of system access for terminated employees?

- ☐ Human resources
- ☐ Legal
- ☐ Help desk
- ☐ Information security

Question 305

Which of the following actions should be taken when an online trading company discovers a network attack in progress?

- ☐ Shut off all network access points
- ☐ Dump all event logs to removable media
- ☐ Isolate the affected network segment
- ☐ Enable trace logging on all event

Question 306

Which of the following is the GREATEST potential exposure created by outsourcing to an application service provider?

- ☐ Denial of service attacks
- ☐ Combining incompatible duties
- ☐ Mixing of data
- ☐ Lack of technical expertise

Question 307

An outcome of effective security governance is:

- ☐ business dependency assessment
- ☐ strategic alignment.
- ☐ risk assessment.
- ☐ planning.

Question 308

Which of the following is the MOST appropriate board-level activity for information security governance?

- ☐ Establish security and continuity ownership
- ☐ Develop “what-if” scenarios on incidents
- ☐ Establish measures for security baselines
- ☐ Include security in job-performance appraisals

Question 309

Risk identification, analysis, and mitigation activities can BEST be integrated into business life cycle processes by linking them to:

- ☐ compliance testing
- ☐ configuration management
- ☐ continuity planning
- ☐ change management

Question 310

Nonrepudiation can BEST be ensured by using:

- ☐ strong passwords.
- ☐ a digital hash.
- ☐ symmetric encryption.
- ☐ digital signatures.

Question 311

After assessing risk, the decision to treat the risk should be based PRIMARILY on:

- ☐ availability of financial resources.
- ☐ whether the level of risk exceeds risk appetite.
- ☐ whether the level of risk exceeds inherent risk.
- ☐ the criticality of the risk.

Question 312

The MAIN reason why asset classification is important to a successful information security program is because classification determines:

- ☐ the priority and extent of risk mitigation efforts.
- ☐ the amount of insurance needed in case of loss.
- ☐ the appropriate level of protection to the asset.
- ☐ how protection levels compare to peer organizations.

Question 313

Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

- ☐ User assessments of changes
- ☐ Comparison of the program results with industry standards
- ☐ Assignment of risk within the organization
- ☐ Participation by all members of the organization

Question 314

A successful risk management program should lead to:

- ☐ optimization of risk reduction efforts against cost.
- ☐ containment of losses to an annual budgeted amount.
- ☐ identification and removal of all man-made threats.
- ☐ elimination or transference of all organizational risks.

Question 315

Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

- ☐ Boundary router
- ☐ Strong encryption
- ☐ Internet-facing firewall
- ☐ Intrusion detection system (IDS)

Question 316

Which of the following would generally have the GREATEST negative impact on an organization?

- ☐ Theft of computer software
- ☐ Interruption of utility services
- ☐ Loss of customer confidence
- ☐ Internal fraud resulting in monetary loss

Question 317

The objective of risk management is to reduce risk to the minimum level that is:

- ☐ compliant with security policies
- ☐ practical given industry and regulatory environments.
- ☐ achievable from technical and financial perspectives.
- ☐ acceptable given the preference of the organization.

Question 318

When security policies are strictly enforced, the initial impact is that:

- ☐ they may have to be modified more frequently.
- ☐ they will be less subject to challenge.
- ☐ the total cost of security is increased.
- ☐ the need for compliance reviews is decreased.

Question 319

To ensure the information security of outsourced IT services, which of the following is the MOST critical due diligence activity?

- ☐ Review samples of service level reports from the service provider.
- ☐ Assess the level of security awareness of the service provider.
- ☐ Request that the service provider comply with information security policy.
- ☐ Review the security status of the service provider.

Question 320

What is an appropriate frequency for updating operating system (OS) patches on production servers?

- ☐ During scheduled rollouts of new applications
- ☐ According to a fixed security patch management schedule
- ☐ Concurrently with quarterly hardware maintenance
- ☐ Whenever important security patches are released

Question 321

Which of the following is MOST effective in preventing security weaknesses in operating systems?

- ☐ Patch management
- ☐ Change management
- ☐ Security baselines
- ☐ Configuration management

Question 322

An organization has implemented an enterprise resource planning (ERP) system used by 500 employees from various departments. Which of the following access control approaches is MOST appropriate?

- ☐ Rule-based
- ☐ Mandatory
- ☐ Discretionary
- ☐ Role-based

Question 323

The BEST way to mitigate the risk associated with a social engineering attack is to:

- ☐ deploy an effective intrusion detection system (IDS).
- ☐ perform a business risk assessment of the email filtering system.
- ☐ implement multi-factor authentication on critical business systems.
- ☐ perform a user-knowledge gap assessment of information security practices.

Question 324

Who can BEST approve plans to implement an information security governance framework?

- ☐ Internal auditor
- ☐ Information security management
- ☐ Steering committee
- ☐ Infrastructure management

Question 325

Senior management has expressed concern that the organization's intrusion prevention system may repeatedly disrupt business operations. Which of the following BEST indicates that the information security manager has tuned the system to address this concern?

- ☐ Decreasing false positives
- ☐ Decreasing false negatives
- ☐ Increasing false positives
- ☐ Increasing false negatives

Question 326

The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

- ☐ Data owner
- ☐ Data custodian
- ☐ Systems programmer
- ☐ Security administrator

Question 327

Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

- ☐ Include security responsibilities in the job description
- ☐ Require the administrator to obtain security certification
- ☐ Train the system administrator on penetration testing and vulnerability assessment
- ☐ Train the system administrator on risk assessment

Question 328

Which of the following provides the MOST comprehensive understanding of an organization's information security posture?

- ☐ Risk management metrics
- ☐ External audit findings
- ☐ Results of vulnerability assessments
- ☐ The organization's security incident trends

Question 329

The PRIMARY goal in developing an information security strategy is to:

- ☐ establish security metrics and performance monitoring.
- ☐ educate business process owners regarding their duties.
- ☐ ensure that legal and regulatory requirements are met
- ☐ support the business objectives of the organization.

Question 330

Which of the following is an important criterion for developing effective key risk indicators (KRIs) to monitor information security risk?

- ☐ The indicator should possess a high correlation with a specific risk and be measured on a regular basis.
- ☐ The indicator should focus on IT and accurately represent risk variances.
- ☐ The indicator should align with key performance indicators and measure root causes of process performance issues.
- ☐ The indicator should provide a retrospective view of risk impacts and be measured annually.

Question 331

Which of the following is the initial step in creating a firewall policy?

- ☐ A cost-benefit analysis of methods for securing the applications
- ☐ Identification of network applications to be externally accessed
- ☐ Identification of vulnerabilities associated with network applications to be externally accessed
- ☐ Creation of an applications traffic matrix showing protection methods

Question 332

An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

- ☐ eliminating the risk.
- ☐ transferring the risk.
- ☐ mitigating the risk.
- ☐ accepting the risk.

Question 333

A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. Which of the following should be performed FIRST in response to this threat?

- ☐ Quarantine all picture files stored on file servers
- ☐ Block all e-mails containing picture file attachments
- ☐ Quarantine all mail servers connected to the Internet
- ☐ Block incoming Internet mail, but permit outgoing mail

Question 334

Which of the following is the BEST approach to identify noncompliance issues with legal, regulatory, and contractual requirements?

- ☐ Risk assessment
- ☐ Business impact analysis (BIA)
- ☐ Vulnerability assessment
- ☐ Gap analysis

Question 335

Which of the following would be the MOST effective to mitigate the risk of data loss in the event of a stolen laptop?

- ☐ Providing end-user awareness training focused on travelling with laptops
- ☐ Deploying end-point data loss prevention software on the laptop
- ☐ Encrypting the hard drive
- ☐ Utilizing a strong password

Question 336

An information security manager has been asked to determine whether an information security initiative has reduced risk to an acceptable level. Which of the following activities would provide the BEST information for the information security manager to draw a conclusion?

- ☐ Initiating a cost-benefit analysis of the implemented controls
- ☐ Reviewing the risk register
- ☐ Conducting a business impact analysis (BIA)
- ☐ Performing a risk assessment

Question 337

Which of the following would be MOST effective in successfully implementing restrictive password policies?

- ☐ Regular password audits
- ☐ Single sign-on system
- ☐ Security awareness program
- ☐ Penalties for noncompliance

Question 338

Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

- ☐ Signal strength
- ☐ Number of administrators
- ☐ Bandwidth
- ☐ Encryption strength

Question 339

Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?

- ☐ Business impact analysis
- ☐ Organizational risk appetite
- ☐ Independent security audit
- ☐ Security risk assessment

Question 340

After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

- ☐ transferred.
- ☐ treated.
- ☐ accepted.
- ☐ terminated.

Question 341

Which of the following is the MOST important consideration when deciding whether to continue outsourcing to a managed security service provider?

- ☐ The business need for the function
- ☐ The cost of the services
- ☐ The vendor's reputation in the industry
- ☐ The ability to meet deliverables

Question 342

Of the following, the BEST method for ensuring that temporary employees do not receive excessive access rights is:

- ☐ mandatory access controls.
- ☐ discretionary access controls.
- ☐ lattice-based access controls.
- ☐ role-based access controls.

Question 343

Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

- ☐ Number of controls implemented
- ☐ Percent of control objectives accomplished
- ☐ Percent of compliance with the security policy
- ☐ Reduction in the number of reported security incidents

Question 344

In order to ensure separation of duties, which of the following activities is BEST performed by someone other than the system administrator?

- ☐ Deleting system logs
- ☐ Using system utilities
- ☐ Monitoring system utilization
- ☐ Defining system recovery procedures

Question 345

Which of the following provides the BEST indication that the information security program is in alignment with enterprise requirements?

- ☐ The security strategy is benchmarked with similar organizations.
- ☐ The information security manager reports to the chief executive officer.
- ☐ Security strategy objectives are defined in business terms.
- ☐ An IT governance committee is in place.

Question 346

An information security manager uses security metrics to measure the:

- ☐ performance of the information security program.
- ☐ performance of the security baseline.
- ☐ effectiveness of the security risk analysis.
- ☐ effectiveness of the incident response team.

Question 347

Which of the following is the BEST approach to make strategic information security decisions?

- ☐ Establish an information security steering committee.
- ☐ Establish periodic senior management meetings.
- ☐ Establish regular information security status reporting.
- ☐ Establish business unit security working groups.

Question 348

In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

- ☐ volume of sensitive data.
- ☐ recovery point objective (RPO).
- ☐ recovery time objective (RTO).
- ☐ interruption window.

Question 349

What is the BEST way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

- ☐ Perform periodic penetration testing
- ☐ Establish minimum security baselines
- ☐ Implement vendor default settings
- ☐ Install a honeypot on the network

Question 350

In order to highlight to management, the importance of network security, the security manager should FIRST:

- ☐ develop a security architecture.
- ☐ install a network intrusion detection system (NIDS) and prepare a list of attacks.
- ☐ develop a network security policy.
- ☐ conduct a risk assessment.

Question 351

A business previously accepted the risk associated with a zero-day vulnerability. The same vulnerability was recently exploited in a high-profile attack on another organization in the same industry. Which of the following should be the information security manager's FIRST course of action?

- ☐ Reassess the risk in terms of likelihood and impact
- ☐ Develop best and worst case scenarios
- ☐ Report the breach of the other organization to senior management
- ☐ Evaluate the cost of remediating the vulnerability

Question 352

The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

- ☐ perform penetration testing.
- ☐ establish security baselines.
- ☐ implement vendor default settings.
- ☐ link policies to an independent standard.

Question 353

Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center?"

- ☐ Mantrap
- ☐ Biometric lock
- ☐ Closed-circuit television (CCTV)
- ☐ Security guard

Question 354

A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

- ☐ meet with stakeholders to decide how to comply.
- ☐ analyze key risks in the compliance process.
- ☐ assess whether existing controls meet the regulation.
- ☐ update the existing security/privacy policy.

Question 355

Priority should be given to which of the following to ensure effective implementation of information security governance?

- ☐ Consultation
- ☐ Negotiation
- ☐ Facilitation
- ☐ Planning

Question 356

What is the MAIN reason for an organization to develop an incident response plan?

- ☐ Trigger immediate recovery procedures.
- ☐ Identify training requirements for the incident response team.
- ☐ Prioritize treatment based on incident criticality.
- ☐ Provide a process for notifying stakeholders of the incident.

Question 357

What should be an information security manager's FIRST course of action when an organization is subject to a new regulatory requirement?

- ☐ Perform a gap analysis
- ☐ Complete a control assessment
- ☐ Submit a business case to support compliance
- ☐ Update the risk register

Question 358

Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

- ☐ Database administrator (DBA)
- ☐ Finance department management
- ☐ Information security manager
- ☐ IT department management

Question 359

In business critical applications, where shared access to elevated privileges by a small group is necessary, the BEST approach to implement adequate segregation of duties is to:

- ☐ ensure access to individual functions can be granted to individual users only.
- ☐ implement role-based access control in the application.
- ☐ enforce manual procedures ensuring separation of conflicting duties.
- ☐ create service accounts that can only be used by authorized team members.

Question 360

A business impact analysis (BIA) is the BEST tool for calculating:

- ☐ total cost of ownership.
- ☐ priority of restoration.
- ☐ annualized loss expectancy (ALE).
- ☐ residual risk.

Question 361

What is the PRIMARY purpose of an unannounced disaster recovery exercise?

- ☐ To evaluate how personnel react to the situation
- ☐ To provide metrics to senior management
- ☐ To estimate the recovery time objective (RTO)
- ☐ To assess service level agreements (SLAs)

Question 362

Which of the following is the MOST important consideration in a bring your own device (BYOD) program to protect company data in the event of a loss?

- ☐ The ability to remotely locate devices
- ☐ The ability to centrally manage devices
- ☐ The ability to restrict unapproved applications
- ☐ The ability to classify types of devices

Question 363

Which of the following will provide the MOST guidance when deciding the level of protection for an information asset?

- ☐ Cost of controls
- ☐ Cost to replace
- ☐ Classification of information
- ☐ Impact to business function

Question 364

An organization is developing a disaster recovery plan for a data center that hosts multiple applications. The application recovery sequence would BEST be determined through an analysis of:

- ☐ Key performance indicators (KPIs)
- ☐ Recovery time objectives (RTOs)
- ☐ Recovery point objectives (RPOs)
- ☐ The data classification scheme

Question 365

Which of the following should be done FIRST when establishing security measures for personal data stored and processed on a human resources management system?

- ☐ Conduct a privacy impact assessment.
- ☐ Evaluate data encryption technologies.
- ☐ Move the system into a separate network.
- ☐ Conduct a vulnerability assessment.

Question 366

An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

- ☐ Key performance indicators (KPIs)
- ☐ Business impact analysis (BIA)
- ☐ Gap analysis
- ☐ Technical vulnerability assessment

Question 367

Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

- ☐ Implement countermeasures.
- ☐ Eliminate the risk.
- ☐ Transfer the risk.
- ☐ Accept the risk.

Question 368

A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

- ☐ Understand the business requirements of the developer portal
- ☐ Perform a vulnerability assessment of the developer portal
- ☐ Install an intrusion detection system (IDS)
- ☐ Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

Question 369

Which of the following is the MOST appropriate individual to implement and maintain the level of information security needed for a specific business application?

- ☐ System analyst
- ☐ Quality control manager
- ☐ Process owner
- ☐ Information security manager

Question 370

An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the BEST assurance that the third party's contract programmers comply with the organization's security policies?

- ☐ Require annual signed agreements of adherence to security policies.
- ☐ Include penalties for noncompliance in the contracting agreement.
- ☐ Perform periodic security assessments of the contractors' activities.
- ☐ Conduct periodic vulnerability scans of the application.

Question 371

In order to highlight to management, the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

- ☐ prepare a security budget.
- ☐ conduct a risk assessment.
- ☐ develop an information security policy.
- ☐ obtain benchmarking information.

Question 372

A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the GREATEST weakness in recovery capability?

- ☐ Exclusive use of the hot site is limited to six weeks
- ☐ The hot site may have to be shared with other customers
- ☐ The time of declaration determines site access priority
- ☐ The provider services all major companies in the area

Question 373

Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

- ☐ An emerging technologies strategy is in place
- ☐ An effective security risk management process is established
- ☐ End user acceptance of emerging technologies is established
- ☐ A cost-benefit analysis process is easier to perform

Question 374

Which of the following is the MOST important requirement for the successful implementation of security governance?

- ☐ Implementing a security balanced scorecard
- ☐ Performing an enterprise-wide risk assessment
- ☐ Mapping to organizational strategies
- ☐ Aligning to an international security framework

Question 375

Which of the following will BEST protect an organization from internal security attacks?

- ☐ Static IP addressing
- ☐ Internal address translation
- ☐ Prospective employee background checks
- ☐ Employee awareness certification program

Question 376

Which of the following is the MOST important reason why information security objectives should be defined?

- ☐ Tool for measuring effectiveness
- ☐ General understanding of goals
- ☐ Consistency with applicable standards
- ☐ Management sign-off and support initiatives

Question 377

In implementing information security governance, the information security manager is PRIMARILY responsible for:

- ☐ developing the security strategy.
- ☐ reviewing the security strategy.
- ☐ communicating the security strategy.
- ☐ approving the security strategy

Question 378

Which of the following is MOST helpful in integrating information security governance with corporate governance?

- ☐ Assigning the implementation of information security governance to the steering committee.
- ☐ Including information security processes within operational and management processes.
- ☐ Providing independent reports of information security efficiency and effectiveness to the board.
- ☐ Aligning the information security governance to a globally accepted framework.

Question 379

Employees in a large multinational organization frequently travel among various geographic locations. Which type of authorization policy BEST addresses this practice?

- ☐ Multilevel
- ☐ Identity
- ☐ Role-based
- ☐ Discretionary

Question 380

Who should drive the risk analysis for an organization?

- ☐ Senior management
- ☐ Security manager
- ☐ Quality manager
- ☐ Legal department

Question 381

An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

- ☐ Unsure that critical data on the server are backed up.
- ☐ Shut down the compromised server.
- ☐ Initiate the incident response process.
- ☐ Shut down the network.

Question 382

Which of the following devices should be placed within a DMZ?

- ☐ Router
- ☐ Firewall
- ☐ Mail relay
- ☐ Authentication server

Question 383

During the security review of a legacy business application, it was discovered that sensitive client data is not encrypted in storage, which does not comply with the organization's information security policy. Which of the following would be the information security manager's BEST course of action?

- ☐ Implement encryption on client data.
- ☐ Report the noncompliance to senior management.
- ☐ Analyze compensating controls and assess the associated risk.
- ☐ Determine the cost of encryption and discuss with the application owner.

Question 384

Mitigating technology risks to acceptable levels should be based PRIMARILY upon:

- ☐ business process reengineering.
- ☐ business process requirement.
- ☐ legal and regulatory requirements.
- ☐ information security budget.

Question 385

Which of the following is the MOST important factor to ensure information security is meeting the organization's objectives?

- ☐ Internal audit's involvement in the security process
- ☐ Implementation of a control self-assessment process
- ☐ Establishment of acceptable risk thresholds
- ☐ Implementation of a security awareness program

Question 386

When a departmental system continues to be out of compliance with an information security policy's password strength requirements, the BEST action to undertake is to:

- ☐ submit the issue to the steering committee.
- ☐ conduct an impact analysis to quantify the risks.
- ☐ isolate the system from the rest of the network.
- ☐ request a risk acceptance from senior management.

Question 387

Which of the following is MOST important when conducting a forensic investigation?

- ☐ Documenting analysis steps
- ☐ Capturing full system images
- ☐ Maintaining a chain of custody
- ☐ Analyzing system memory

Question 388

Ensuring that an organization can conduct security reviews within third-party facilities is PRIMARILY enabled by:

- ☐ service level agreements (SLAs)
- ☐ acceptance of the organization's security policies
- ☐ contractual agreements
- ☐ audit guidelines

Question 389

A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?

- ☐ Authority of the subscriber to approve access to its data
- ☐ Right of the subscriber to conduct onsite audits of the vendor
- ☐ Escrow of software code with conditions for code release
- ☐ Comingling of subscribers' data on the same physical server

Question 390

Successful implementation of information security governance will FIRST require:

- ☐ security awareness training.
- ☐ updated security policies.
- ☐ a computer incident management team.
- ☐ a security architecture.

Question 391

The MOST important reason for formally documenting security procedures is to ensure:

- ☐ processes are repeatable and sustainable.
- ☐ alignment with business objectives.
- ☐ auditability by regulatory agencies.
- ☐ objective criteria for the application of metrics.

Question 392

Security awareness training should be provided to new employees:

- ☐ on an as-needed basis.
- ☐ during system user training.
- ☐ before they have access to data.
- ☐ along with department staff.

Question 393

What is the BEST way to ensure data protection upon termination of employment?

- ☐ Retrieve identification badge and card keys
- ☐ Retrieve all personal computer equipment
- ☐ Erase all of the employee's folders
- ☐ Ensure all logical access is removed

Question 394

A large number of exceptions to an organization's information security standards have been granted after senior management approved a bring your own device (BYOD) program. To address this situation, it is MOST important for the information security manager to:

- ☐ introduce strong authentication on devices.
- ☐ reject new exception requests.
- ☐ update the information security policy.
- ☐ require authorization to wipe lost devices.

Question 395

Which of the following BEST reduces the likelihood of leakage of private information via email?

- ☐ Email encryption
- ☐ User awareness training
- ☐ Strong user authentication protocols
- ☐ Prohibition on the personal use of email

Question 396

A business case for investment in an information security management infrastructure MUST include:

- ☐ evidence that the proposed infrastructure is certified.
- ☐ specifics on the security applications needed.
- ☐ data management methods currently in use.
- ☐ impact of noncompliance with applicable standards.

Question 397

Which of the following would MOST likely require a business continuity plan to be invoked?

- ☐ An unauthorized visitor discovered in the data center
- ☐ A distributed denial of service attack on an e-mail server
- ☐ An epidemic preventing staff from performing job functions
- ☐ A hacker holding personally identifiable information hostage

Question 398

Which of the following is the GREATEST security threat when an organization allows remote access to a virtual private network (VPN)?

- ☐ Client logins are subject to replay attack
- ☐ Compromised VPN clients could impact the network
- ☐ Attackers could compromise the VPN gateway
- ☐ VPN traffic could be sniffed and captured

Question 399

The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:

- ☐ maintain an accurate record of users' access rights.
- ☐ serve as evidence of security awareness training.
- ☐ maintain compliance with industry best practices.
- ☐ assign accountability for transactions made with the user's ID.

Question 400

Which of the following is the BEST reason to initiate a reassessment of current risk?

- ☐ Follow-up to an audit report
- ☐ A recent security incident
- ☐ Certification requirements
- ☐ Changes to security personnel

Question 401

Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

- ☐ Integrating the risk assessment into the internal audit program
- ☐ Applying global security standards to the IT projects
- ☐ Training project managers on risk assessment
- ☐ Having the information security manager participate on the project setting committees

Question 402

Which of the following is the PRIMARY advantage of desk checking a business continuity plan (BCP)?

- ☐ Assesses the availability and compatibility a backup hardware
- ☐ Allows for greater participation be management and the IT department
- ☐ Ensures that appropriate follow-up work is performed on noted issues
- ☐ Provides a low-cost method of assessing the BCP's completeness

Question 403

In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

- ☐ testing time window prior to deployment.
- ☐ technical skills of the team responsible.
- ☐ certification of validity for deployment.
- ☐ automated deployment to all the servers.

Question 404

Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

- ☐ policy.
- ☐ strategy.
- ☐ guideline
- ☐ baseline.

Question 405

Relationships among security technologies are BEST defined through which of the following?

- ☐ Security metrics
- ☐ Network topology
- ☐ Security architecture
- ☐ Process improvement models

Question 406

Which of the following is the BEST approach when using sensitive customer data during the testing phase of a systems development project?

- ☐ Establish the test environment on a separate network.
- ☐ Sanitize customer data.
- ☐ Monitor the test environment for data loss.
- ☐ Implement equivalent controls to those on the source system.

Question 407

Which of the following is the MOST important reason for performing a cost-benefit analysis when implementing a security control?

- ☐ To present a realistic information security budget
- ☐ To ensure that benefits are aligned with business strategies
- ☐ To ensure that the mitigation effort does not exceed the asset value
- ☐ To justify information security program activities

Question 408

Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

- ☐ define the circumstances where cryptography should be used.
- ☐ define cryptographic algorithms and key lengths.
- ☐ describe handling procedures of cryptographic keys.
- ☐ establish the use of cryptographic solutions.

Question 409

Which of the following is the MOST effective mitigation strategy to protect confidential information from insider threats?

- ☐ Performing an entitlement review process
- ☐ Implementing authentication mechanism
- ☐ Defining segregation of duties
- ☐ Establishing authorization controls

Question 410

Which of the following would be MOST helpful when justifying the funding required for a compensating control?

- ☐ Business case
- ☐ Risk analysis
- ☐ Business impact analysis
- ☐ Threat assessment

Question 411

An organization involved in e-commerce activities operating from its home country opened a new office in another country with stringent security laws. In this scenario, the overall security strategy should be based on:

- ☐ risk assessment results.
- ☐ international security standards.
- ☐ the most stringent requirements.
- ☐ the security organization structure.

Question 412

Which of the following activities is MOST likely to increase the difficulty of totally eradicating malicious code that is not immediately detected?

- ☐ Applying patches
- ☐ Changing access rules
- ☐ Upgrading hardware
- ☐ Backing up files

Question 413

What is the BEST way to alleviate security team understaffing while retaining the capability in-house?

- ☐ Hire a contractor that would not be included in the permanent headcount
- ☐ Outsource with a security services provider while retaining the control internally
- ☐ Establish a virtual security team from competent employees across the company
- ☐ Provide cross training to minimize the existing resources gap

Question 414

In the event that a password policy cannot be implemented for a legacy application, which of the following is the BEST course of action?

- ☐ Update the application security policy.
- ☐ Implement compensating control.
- ☐ Submit a waiver for the legacy application.
- ☐ Perform an application security assessment.

Question 415

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

- ☐ Deleting database activity logs
- ☐ Implementing database optimization tools
- ☐ Monitoring database usage
- ☐ Defining backup and recovery procedures

Question 416

Which of the following analyses will BEST identify the external influences to an organization's information security?

- ☐ Gap analysis
- ☐ Business impact analysis
- ☐ Threat analysis
- ☐ Vulnerability analysis.

Question 417

Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

- ☐ Passwords stored in encrypted form
- ☐ User awareness
- ☐ Strong passwords that are changed periodically
- ☐ Implementation of lock-out policies

Question 418

Which of the following are likely to be updated MOST frequently?

- ☐ Procedures for hardening database servers
- ☐ Standards for password length and complexity
- ☐ Policies addressing information security governance
- ☐ Standards for document retention and destruction

Question 419

The MAIN advantage of implementing automated password synchronization is that it:

- ☐ reduces overall administrative workload.
- ☐ increases security between multi-tier systems.
- ☐ allows passwords to be changed less frequently.
- ☐ reduces the need for two-factor authentication.

Question 420

To justify the establishment of an incident management team, an information security manager would find which of the following to be the MOST effective?

- ☐ Assessment of business impact of past incidents
- ☐ Need of an independent review of incident causes
- ☐ Need for constant improvement on the security level
- ☐ Possible business benefits from incident impact reduction

Question 421

In an organization that has undergone an expansion through an acquisition which of the following would BEST secure the enterprise network?

- ☐ Using security groups
- ☐ Log analysis of system access
- ☐ Business or role-based segmentation
- ☐ Encryption of data traversing networks

Question 422

Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

- ☐ Batch patches into frequent server updates
- ☐ Initially load the patches on a test machine
- ☐ Set up servers to automatically download patches
- ☐ Automatically push all patches to the servers

Question 423

Who is MOST important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data loss?

- ☐ An independent auditor for identification of control deficiencies
- ☐ A damage assessment expert for calculating losses
- ☐ A forensics expert for evidence management
- ☐ A penetration tester to validate the attack

Question 424

The recovery point objective (RPO) requires which of the following?

- ☐ Disaster declaration
- ☐ Before-image restoration
- ☐ System restoration
- ☐ After-image processing

Question 425

When designing an information security quarterly report to management, the MOST important element to be considered should be the:

- ☐ information security metrics.
- ☐ knowledge required to analyze each issue.
- ☐ linkage to business area objectives.
- ☐ baseline against which metrics are evaluated.

Question 426

Which of the following would be the MOST important goal of an information security governance program?

- ☐ Review of internal control mechanisms
- ☐ Effective involvement in business decision making
- ☐ Total elimination of risk factors
- ☐ Ensuring trust in data

Question 427

To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRST crucial step an information security manager would take in ensuring business continuity planning?

- ☐ Conducting a qualitative and quantitative risk analysis.
- ☐ Assigning value to the assets.
- ☐ Weighing the cost of implementing the plan vs. financial loss.
- ☐ Conducting a business impact analysis (BIA).

Question 428

After undertaking a security assessment of a production system, the information security manager is MOST likely to:

- ☐ inform the system owner of any residual risks and propose measures to reduce them.
- ☐ inform the development team of any residual risks, and together formulate risk reduction measures.
- ☐ inform the IT manager of the residual risks and propose measures to reduce them.
- ☐ establish an overall security program that minimizes the residual risks of that production system.

Question 429

Which of the following is a MAIN security challenge when conducting a post-incident review related to bring your own device (BYOD) in a mature, diverse organization?

- ☐ Ability to obtain possession of device
- ☐ Lack of mobile forensics expertise
- ☐ Diversity of operating systems
- ☐ Ability to access device remotely

Question 430

When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

- ☐ Compliance with international security standards.
- ☐ Use of a two-factor authentication system.
- ☐ Existence of an alternate hot site in case of business disruption.
- ☐ Compliance with the organization's information security requirements.

Question 431

Isolation and containment measures for a compromised computer has been taken and information security management is now investigating. What is the MOST appropriate next step?

- ☐ Run a forensics tool on the machine to gather evidence
- ☐ Reboot the machine to break remote connections
- ☐ Make a copy of the whole system's memory
- ☐ Document current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/ UDP) ports

Question 432

Successful social engineering attacks can BEST be prevented through:

- ☐ preemployment screening.
- ☐ close monitoring of users' access patterns.
- ☐ periodic awareness training.
- ☐ efficient termination procedures.

Question 433

Which of the following would BEST ensure that application security standards are in place?

- ☐ Functional testing
- ☐ Performing a code review
- ☐ Publishing software coding standards
- ☐ Penetration testing

Question 434

Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

- ☐ Theft of purchased software
- ☐ Power outage lasting 24 hours
- ☐ Permanent decline in customer confidence
- ☐ Temporary loss of e-mail due to a virus attack

Question 435

A common concern with poorly written web applications is that they can allow an attacker to:

- ☐ gain control through a buffer overflow.
- ☐ conduct a distributed denial of service (DoS) attack.
- ☐ abuse a race condition.
- ☐ inject structured query language (SQL) statements.

Question 436

Which of the following would MOST effectively ensure that information security is implemented in a new system?

- ☐ Security baselines
- ☐ Security scanning
- ☐ Secure code reviews
- ☐ Penetration testing

Question 437

Which of the following is the MOST effective way of ensuring that business units comply with an information security governance framework?

- ☐ Integrating security requirements with processes
- ☐ Performing security assessments and gap analysis
- ☐ Conducting a business impact analysis (BIA)
- ☐ Conducting information security awareness training

Question 438

Which of the following is the PRIMARY benefit of implementing a maturity model for information security management?

- ☐ Information security management costs will be optimized.
- ☐ Information security strategy will be in line with industry best practice.
- ☐ Gaps between current and desirable levels will be addressed.
- ☐ Staff awareness of information security compliance will be promoted.

Question 439

When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

- ☐ the information security steering committee.
- ☐ customers who may be impacted.
- ☐ data owners who may be impacted.
- ☐ regulatory- agencies overseeing privacy.

Question 440

An information security manager is advised by contacts in law enforcement that there is evidence that his/ her company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The FIRST step that the security manager should take is to:

- ☐ perform a comprehensive assessment of the organization's exposure to the hacker's techniques.
- ☐ initiate awareness training to counter social engineering.
- ☐ immediately advise senior management of the elevated risk.
- ☐ increase monitoring activities to provide early detection of intrusion.

Question 441

Which of the following is MOST important for the effectiveness of an incident response function?

- ☐ Enterprise security management system and forensic tools.
- ☐ Establishing prior contacts with law enforcement
- ☐ Training of all users on when and how to report
- ☐ Automated incident tracking and reporting tools

Question 442

Which of the following is responsible for legal and regulatory liability?

- ☐ Chief security officer (CSO)
- ☐ Chief legal counsel (CLC)
- ☐ Board and senior management
- ☐ Information security steering group

Question 443

Which of the following would BEST help to identify vulnerabilities introduced by changes to an organization's technical infrastructure?

- ☐ An intrusion detection system
- ☐ Established security baselines
- ☐ Penetration testing
- ☐ Log aggregation and correlation

Question 444

When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

- ☐ Business management
- ☐ Operations manager
- ☐ Information security manager
- ☐ System users

Question 445

What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

- ☐ Authentication
- ☐ Encryption
- ☐ Prohibit employees from copying data to USB devices
- ☐ Limit the use of USB devices

Question 446

Security awareness training is MOST likely to lead to which of the following?

- ☐ Decrease in intrusion incidents
- ☐ Increase in reported incidents
- ☐ Decrease in security policy changes
- ☐ Increase in access rule violations

Question 447

An organization permits the storage and use of its critical and sensitive information on employee-owned smartphones. Which of the following is the BEST security control?

- ☐ Requiring the backup of the organization's data by the user
- ☐ Establishing the authority to remote wipe
- ☐ Monitoring how often the smartphone is used
- ☐ Developing security awareness training

Question 448

An information security manager discovers that newly hired privileged users are not taking necessary steps to protect critical information at their workstations. Which of the following is the BEST way to address this situation?

- ☐ Communicate the responsibility and provide appropriate training.
- ☐ Publish an acceptable use policy and require signed acknowledgment.
- ☐ Turn on logging and record user activity.
- ☐ Implement a data loss prevention (DLP) solution.

Question 449

Organization XYZ, a lucrative, Internet-only business, recently suffered a power outage that lasted two hours. The organization's data center was unavailable in the interim. In order to mitigate risk in the MOST cost-efficient manner, the organization should:

- ☐ plan to operate at a reduced capacity from the primary place of business.
- ☐ create an IT hot site with immediate fail-over capability.
- ☐ install an uninterruptible power supply (UPS) and generator.
- ☐ set up a duplicate business center in a geographically separate area.

Question 450

Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?

- ☐ Effective security eliminates risk to the business
- ☐ Adopt a recognized framework with metrics
- ☐ Security is a business product and not a process
- ☐ Security supports and protects the business

Question 451

Which of the following is the MOST reliable way to ensure network security incidents are identified as soon as possible?

- ☐ Collect and correlate IT infrastructure event logs.
- ☐ Conduct workshops and training sessions with end users.
- ☐ Install stateful inspection firewalls.
- ☐ Train help desk staff to identify and prioritize security incidents.

Question 452

When developing a disaster recovery plan, which of the following would be MOST helpful in prioritizing the order in which systems should be recovered?

- ☐ Performing a business impact analysis
- ☐ Measuring the volume of data in each system
- ☐ Reviewing the information security policy
- ☐ Reviewing the business strategy

Question 453

A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

- ☐ Run a port scan on the system
- ☐ Disable the logon ID
- ☐ Investigate the system logs
- ☐ Validate the incident

Question 454

To justify its ongoing security budget, which of the following would be of MOST use to the information security' department?

- ☐ Security breach frequency
- ☐ Annualized loss expectancy (ALE)
- ☐ Cost-benefit analysis
- ☐ Peer group comparison

Question 455

Which of the following is the BEST indicator that security awareness training has been effective?

- ☐ Employees sign to acknowledge the security policy
- ☐ More incidents are being reported
- ☐ A majority of employees have completed training
- ☐ No incidents have been reported in three months

Question 456

Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

- ☐ Alignment with industry best practices
- ☐ Business continuity investment
- ☐ Business benefits
- ☐ Regulatory compliance

Question 457

The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

- ☐ ensure the provider is made liable for losses.
- ☐ recommend not renewing the contract upon expiration.
- ☐ recommend the immediate termination of the contract.
- ☐ determine the current level of security.

Question 458

To integrate security into system development life cycle (SDLC) processes, an organization MUST ensure that security:

- ☐ is represented on the configuration control board.
- ☐ performance metrics have been met.
- ☐ roles and responsibilities have been defined.
- ☐ is a prerequisite for completion of major phases.

Question 459

Which of the following is the BEST method to defend against social engineering attacks?

- ☐ Periodically perform antivirus scans to identify malware.
- ☐ Communicate guidelines to limit information posted to public sites.
- ☐ Employ the use of a web-content filtering solution.
- ☐ Monitor for unauthorized access attempts and failed logins.

Question 460

The MAIN reason for having the Information Security Steering Committee review a new security controls implementation plan is to ensure that:

- ☐ the plan aligns with the organization's business plan.
- ☐ departmental budgets are allocated appropriately to pay for the plan.
- ☐ regulatory oversight requirements are met.
- ☐ the impact of the plan on the business units is reduced.

Question 461

Which of the following is the MOST important prerequisite for establishing information security management within an organization?

- ☐ Senior management commitment
- ☐ Information security framework
- ☐ Information security organizational structure
- ☐ Information security policy

Question 462

Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

- ☐ it implies compliance risks.
- ☐ short-term impact cannot be determined.
- ☐ it violates industry security practices.
- ☐ changes in the roles matrix cannot be detected.

Question 463

Senior management wants to provide mobile devices to its sales force. Which of the following should the information security manager do FIRST to support this objective?

- ☐ Assess risks introduced by the technology.
- ☐ Develop an acceptable use policy.
- ☐ Conduct a vulnerability assessment on the devices.
- ☐ Research mobile device management (MDM) solutions.

Question 464

Which of the following should be determined FIRST when establishing a business continuity program?

- ☐ Cost to rebuild information processing facilities
- ☐ Incremental daily cost of the unavailability of systems
- ☐ Location and cost of offsite recovery facilities
- ☐ Composition and mission of individual recovery teams

Question 465

How would an organization know if its new information security program is accomplishing its goals?

- ☐ Key metrics indicate a reduction in incident impacts.
- ☐ Senior management has approved the program and is supportive of it.
- ☐ Employees are receptive to changes that were implemented.
- ☐ There is an immediate reduction in reported incidents.

Question 466

The MAIN reason for continuous monitoring of a security strategy is to:

- ☐ optimize resource allocation.
- ☐ confirm benefits are being realized.
- ☐ evaluate the implementation of the strategy.
- ☐ allocate funds for information security

Question 467

When implementing security controls, an information security manager must PRIMARILY focus on:

- ☐ minimizing operational impacts.
- ☐ eliminating all vulnerabilities.
- ☐ usage by similar organizations.
- ☐ certification from a third party.

Question 468

When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?

- ☐ Ensuring accessibility should a disaster occur
- ☐ Versioning control as plans are modified
- ☐ Broken hyperlinks to resources stored elsewhere
- ☐ Tracking changes in personnel and plan assets

Question 469

The MOST important objective of a post incident review is to:

- ☐ capture lessons learned to improve the process.
- ☐ develop a process for continuous improvement.
- ☐ develop a business case for the security program budget.
- ☐ identify new incident management tools.

Question 470

The decision as to whether a risk has been reduced to an acceptable level should be determined by:

- ☐ organizational requirements.
- ☐ information systems requirements.
- ☐ information security requirements.
- ☐ international standards.

Question 471

Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

- ☐ Countermeasure cost-benefit analysis
- ☐ Penetration testing
- ☐ Frequent risk assessment programs
- ☐ Annual loss expectancy (ALE) calculation

Question 472

Which of the following is the BEST way to facilitate the alignment between an organization's information security program and business objectives?

- ☐ Information security is considered at the feasibility stage of all IT projects.
- ☐ The information security governance committee includes representation from key business areas.
- ☐ The chief executive officer reviews and approves the information security program.
- ☐ The information security program is audited by the internal audit department.

Question 473

When developing an information security governance framework, which of the following would be the MAIN impact when lacking senior management involvement?

- ☐ Accountability for risk treatment is not clearly defined.
- ☐ Information security responsibilities are not communicated effectively.
- ☐ Resource requirements are not adequately considered.
- ☐ Information security plans do not support business requirements.

Question 474

Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?

- ☐ Escalation processes
- ☐ Security audit reports
- ☐ Technological capabilities
- ☐ Recovery time objective (RTO)

Question 475

What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

- ☐ Periodic review of network configuration
- ☐ Review intrusion detection system (IDS) logs for evidence of attacks
- ☐ Periodically perform penetration tests
- ☐ Daily review of server logs for evidence of hacker activity

Question 476

The BEST way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

- ☐ simulate an attack and review IDS performance.
- ☐ use a honeypot to check for unusual activity.
- ☐ audit the configuration of the IDS.
- ☐ benchmark the IDS against a peer site.

Question 477

An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

- ☐ Security in storage and transmission of sensitive data
- ☐ Provider's level of compliance with industry standards
- ☐ Security technologies in place at the facility
- ☐ Results of the latest independent security review

Question 478

An information security organization should PRIMARILY:

- ☐ support the business objectives of the company by providing security-related support services.
- ☐ be responsible for setting up and documenting the information security responsibilities of the information security team members.
- ☐ ensure that the information security policies of the company are in line with global best practices and standards.
- ☐ ensure that the information security expectations are conveyed to employees.

Question 479

A newly hired information security manager reviewing an existing security investment plan is MOST likely to be concerned when the plan:

- ☐ is based solely on a review of security threats and vulnerabilities in existing IT systems
- ☐ identifies potential impacts that the implementation may have on business processes
- ☐ focuses on compliance with common international security standards
- ☐ has summarized IT costs for implementation rather than providing detail

Question 480

Which of the following is the MOST important reason for performing vulnerability assessments periodically?

- ☐ Management requires regular reports.
- ☐ The environment changes constantly.
- ☐ Technology risks must be mitigated.
- ☐ The current threat levels are being assessed.

Question 481

Which of the following would BEST justify spending for a compensating control?

- ☐ Threat analysis
- ☐ Risk analysis
- ☐ Peer benchmarking
- ☐ Vulnerability analysis

Question 482

Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

- ☐ The program's governance oversight mechanisms
- ☐ Information security periodicals and manuals
- ☐ The program's security architecture and design
- ☐ Training and certification of the information security team

Question 483

An organization has a policy in which all criminal activity is prosecuted. What is MOST important for the information security manager to ensure when an employee is suspected of using a company computer to commit fraud?

- ☐ The forensics process is immediately initiated
- ☐ The incident response plan is initiated
- ☐ The employee's log files are backed-up
- ☐ Senior management is informed of the situation

Question 484

Which of the following is the BEST justification to convince management to invest in an information security program?

- ☐ Cost reduction
- ☐ Compliance with company policies
- ☐ Protection of business assets
- ☐ Increased business value

Question 485

When developing a new system, detailed information security functionality should FIRST be addressed:

- ☐ as part of prototyping.
- ☐ during the system design phase.
- ☐ when system requirements are defined.
- ☐ as part of application development.

Question 486

Risk assessment should be conducted on a continuing basis because:

- ☐ controls change on a continuing basis
- ☐ the number of hacking incidents is increasing
- ☐ management should be updated about changes in risk
- ☐ factors that affect information security change

Question 487

The effectiveness of an information security governance framework will BEST be enhanced if:

- ☐ IS auditors are empowered to evaluate governance activities
- ☐ risk management is built into operational and strategic activities
- ☐ a culture of legal and regulatory compliance is promoted by management
- ☐ consultants review the information security governance framework

Question 488

Which of the following controls would BEST prevent accidental system shutdown from the console or operations area?

- ☐ Redundant power supplies
- ☐ Protective switch covers
- ☐ Shutdown alarms
- ☐ Biometric readers

Question 489

When developing an incident response plan, the information security manager should:

- ☐ include response scenarios that have been approved previously by business management.
- ☐ determine recovery time objectives (RTOs).
- ☐ allow IT to decide which systems can be removed from the infrastructure.
- ☐ require IT to invoke the business continuity plan.

Question 490

The BEST way to minimize errors in the response to an incident is to:

- ☐ follow standard operating procedures.
- ☐ analyze the situation during the incident.
- ☐ implement vendor recommendations.
- ☐ reference system administration manuals.

Question 491

Which of the following is an example of a corrective control?

- ☐ Diverting incoming traffic upon responding to the denial of service (DoS) attack
- ☐ Filtering network traffic before entering an internal network from outside
- ☐ Examining inbound network traffic for viruses
- ☐ Logging inbound network traffic

Question 492

Which of the following is the PRIMARY reason to conduct periodic business impact assessments?

- ☐ Improve the results of last business impact assessment
- ☐ Update recovery objectives based on new risks
- ☐ Decrease the recovery times
- ☐ Meet the needs of the business continuity policy

Question 493

When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

- ☐ calculating the residual risk.
- ☐ enforcing the security standard.
- ☐ redesigning the system change.
- ☐ implementing mitigating controls.

Question 494

What is the BEST way to determine the level of risk associated with information assets processed by an IT application?

- ☐ Evaluate the potential value of information for an attacker
- ☐ Calculate the business value of the information assets
- ☐ Review the cost of acquiring the information assets for the business
- ☐ Research compliance requirements associated with the information

Question 495

Which of the following is the BEST method to ensure that data owners take responsibility for implementing information security processes?

- ☐ Include security tasks into employee job descriptions.
- ☐ Include membership on project teams.
- ☐ Provide job rotation into the security organization.
- ☐ Increase security awareness training.

Question 496

The data access requirements for an application should be determined by the:

- ☐ legal department.
- ☐ compliance officer.
- ☐ information security manager.
- ☐ business owner.

Question 497

During the restoration of several servers, a critical process that services external customers was restored late due to a failure, resulting in lost revenue. Which of the following would have BEST help to prevent this occurrence?

- ☐ Validation of senior management's risk tolerance
- ☐ Updates to the business impact analysis (BIA)
- ☐ More effective disaster recovery plan (DRP) testing
- ☐ Improvements to incident identification methods

Question 498

What is the BEST course of action when an information security manager finds an external service provider has not implemented adequate controls for safeguarding the organization's critical data?

- ☐ Assess the impact of the control gap.
- ☐ Initiate contract renegotiations.
- ☐ Purchase additional insurance.
- ☐ Conduct a controls audit of the provider.

Question 499

Which of the following presents the GREATEST exposure to internal attack on a network?

- ☐ User passwords are not automatically expired
- ☐ All network traffic goes through a single switch
- ☐ User passwords are encoded but not encrypted
- ☐ All users reside on a single internal subnet

Question 500

The BEST strategy for risk management is to:

- ☐ achieve a balance between risk and organizational goals.
- ☐ reduce risk to an acceptable level.
- ☐ ensure that policy development properly considers organizational risks.
- ☐ ensure that all unmitigated risks are accepted by management.

Question 501

From an information security manager perspective, what is the immediate benefit of clearly-defined roles and responsibilities?

- ☐ Enhanced policy compliance
- ☐ Improved procedure flows
- ☐ Segregation of duties
- ☐ Better accountability

Question 502

An information security manager's PRIMARY objective for presenting key risks to the board of directors is to:

- ☐ meet information security compliance requirements.
- ☐ ensure appropriate information security governance.
- ☐ quantify reputational risks.
- ☐ re-evaluate the risk appetite.

Question 503

A risk management program would be expected to:

- ☐ remove all inherent risk.
- ☐ maintain residual risk at an acceptable level.
- ☐ implement preventive controls for every threat.
- ☐ reduce control risk to zero.

Question 504

Several significant risks have been identified after a centralized risk register was compiled and prioritized. The information security manager's most important action is to:

- ☐ provide senior management with risk treatment options.
- ☐ design and implement controls to reduce the risk.
- ☐ consult external third parties on how to treat the risk.
- ☐ ensure that employees are aware of the risk.

Question 505

Which of the following is the PRIMARY responsibility of the designated spokesperson during incident response testing?

- ☐ Communicating the severity of the incident to the board
- ☐ Establishing communication channels throughout the organization
- ☐ Evaluating the effectiveness of the communication processes
- ☐ Acknowledging communications from the incident response team

Question 506

An organization shares customer information across its globally dispersed branches. Which of the following should be the GREATEST concern to information security management?

- ☐ Cross-cultural differences between branches
- ☐ Conflicting data protection regulations
- ☐ Insecure wide area networks (WANs)
- ☐ Decentralization of information security

Question 507

The security responsibility of data custodians in an organization will include:

- ☐ assuming overall protection of information assets.
- ☐ determining data classification levels.
- ☐ implementing security controls in products they install.
- ☐ ensuring security measures are consistent with policy.

Question 508

Which of the following is the BEST indicator that an effective security control is built into an organization?

- ☐ The monthly service level statistics indicate a minimal impact from security issues.
- ☐ The cost of implementing a security control is less than the value of the assets.
- ☐ The percentage of systems that is compliant with security standards.
- ☐ The audit reports do not reflect any significant findings on security.

Question 509

The PRIMARY reason for assigning classes of sensitivity and criticality to information resources is to provide a basis for:

- ☐ determining the scope for inclusion in an information security program.
- ☐ defining the level of access controls.
- ☐ justifying costs for information resources.
- ☐ determining the overall budget of an information security program.

Question 510

Which of the following has the GREATEST influence on an organization's information security strategy?

- ☐ The organization's risk tolerance
- ☐ The organizational structure
- ☐ Information security awareness
- ☐ Industry security standards

Question 511

An information security manager has developed a strategy to address new information security risks resulting from recent changes in the business. Which of the following would be MOST important to include when presenting the strategy to senior management?

- ☐ The costs associated with business process changes
- ☐ Results of benchmarking against industry peers
- ☐ The impact of organizational changes on the security risk profile
- ☐ Security controls needed for risk mitigation

Question 512

Who is responsible for raising awareness of the need for adequate funding for risk action plans?

- ☐ Chief information officer (CIO)
- ☐ Chief financial officer (CFO)
- ☐ Information security manager
- ☐ Business unit management

Question 513

Which of the following should be determined while defining risk management strategies?

- ☐ Risk assessment criteria
- ☐ Organizational objectives and risk appetite
- ☐ IT architecture complexity
- ☐ Enterprise disaster recovery plans

Question 514

Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

- ☐ Biometric authentication
- ☐ Embedded steganographic
- ☐ Two-factor authentication
- ☐ Embedded digital signature

Question 515

An incident response team has determined there is a need to isolate a system that is communicating with a known malicious host on the Internet.

Which of the following stakeholders should be contacted FIRST?

- ☐ Executive management
- ☐ System administrator
- ☐ Key customers
- ☐ The business owner

Question 516

Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:

- ☐ ensure the controls are regularly tested for ongoing effectiveness.
- ☐ hand over the controls to the relevant business owners.
- ☐ prepare to adapt the controls for future system upgrades.
- ☐ perform testing to compare control performance against industry levels.

Question 517

When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

- ☐ Evaluate productivity losses
- ☐ Assess the impact of confidential data disclosure
- ☐ Calculate the value of the information or asset
- ☐ Measure the probability of occurrence of each threat

Question 518

The PRIMARY purpose of vulnerability assessments is to:

- ☐ determine the impact of potential threats.
- ☐ test intrusion detection systems (IDS) and response procedures.
- ☐ provide clear evidence that the system is sufficiently secure.
- ☐ detect deficiencies that could lead to a system compromise.

Question 519

An organization's information security strategy should be based on:

- ☐ managing risk relative to business objectives.
- ☐ managing risk to a zero level and minimizing insurance premiums.
- ☐ avoiding occurrence of risks so that insurance is not required.
- ☐ transferring most risks to insurers and saving on control costs.

Question 520

The PRIMARY reason for initiating a policy exception process is when:

- ☐ operations are too busy to comply.
- ☐ the risk is justified by the benefit.
- ☐ policy compliance would be difficult to enforce.
- ☐ users may initially be inconvenienced.

Question 521

An information security manager has been informed of a new vulnerability in an online banking application, and patch to resolve this issue is expected to be released in the next 72 hours. The information security manager's MOST important course of action should be to:

- ☐ assess the risk and advise senior management.
- ☐ identify and implement mitigating controls.
- ☐ run the application system in offline mode.
- ☐ perform a business impact analysis (BIA).

Question 522

Several business units reported problems with their systems after multiple security patches were deployed. The FIRST step in handling this problem would be to:

- ☐ assess the problems and institute rollback procedures, if needed.
- ☐ disconnect the systems from the network until the problems are corrected.
- ☐ immediately uninstall the patches from these systems.
- ☐ immediately contact the vendor regarding the problems that occurred.

Question 523

Which of the following would a security manager establish to determine the target for restoration of normal processing?

- ☐ Recover time objective (RTO)
- ☐ Maximum tolerable outage (MTO)
- ☐ Recovery point objectives (RPOs)
- ☐ Services delivery objectives (SDOs)

Question 524

Which of the following is the MOST appropriate use of gap analysis?

- ☐ Evaluating a business impact analysis (BIA)
- ☐ Developing a balanced business scorecard
- ☐ Demonstrating the relationship between controls
- ☐ Measuring current state vs. desired future state

Question 525

Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

- ☐ Strong authentication by password
- ☐ Encrypted hard drives
- ☐ Multifactor authentication procedures
- ☐ Network-based data backup

Question 526

The PRIMARY objective of an Internet usage policy is to prevent:

- ☐ access to inappropriate sites.
- ☐ downloading malicious code.
- ☐ violation of copyright laws.
- ☐ disruption of Internet access.

Question 527

Which of the following areas is MOST susceptible to the introduction of security weaknesses?

- ☐ Database management
- ☐ Tape backup management
- ☐ Configuration management
- ☐ Incident response management

Question 528

Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

- ☐ Obtain the support of the board of directors.
- ☐ Improve the content of the information security awareness program.
- ☐ Improve the employees' knowledge of security policies.
- ☐ Implement logical access controls to the information systems.

Question 529

Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

- ☐ Periodic focus group meetings
- ☐ Periodic compliance reviews
- ☐ Computer-based certification training (CBT)
- ☐ Employee's signed acknowledgement

Question 530

The cost of implementing a security control should not exceed the:

- ☐ annualized loss expectancy.
- ☐ cost of an incident.
- ☐ asset value.
- ☐ implementation opportunity costs.

Question 531

An organization with a large number of users finds it necessary to improve access control applications. Which of the following would BEST help to prevent unauthorized user access to networks and applications?

- ☐ Single sign-on
- ☐ Biometric systems
- ☐ Complex user passwords
- ☐ Access control lists

Question 532

An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

- ☐ Right to audit
- ☐ Nondisclosure agreement
- ☐ Proper firewall implementation
- ☐ Dedicated security manager for monitoring compliance

Question 533

A message* that has been encrypted by the sender's private key and again by the receiver's public key achieves:

- ☐ authentication and authorization.
- ☐ confidentiality and integrity.
- ☐ confidentiality and nonrepudiation.
- ☐ authentication and nonrepudiation.

Question 534

Which of the following steps should be performed FIRST in the risk assessment process?

- ☐ Staff interviews
- ☐ Threat identification
- ☐ Asset identification and valuation
- ☐ Determination of the likelihood of identified risks

Question 535

A new system has been developed that does not comply with password-aging rules. This noncompliance can BEST be identified through:

- ☐ a business impact analysis
- ☐ an internal audit assessment
- ☐ an incident management process
- ☐ a progressive series of warnings

Question 536

When defining a service level agreement (SLA) regarding the level of data confidentiality that is handled by a third-party service provider, the BEST indicator of compliance would be the:

- ☐ access control matrix.
- ☐ encryption strength.
- ☐ authentication mechanism.
- ☐ data repository.

Question 537

An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

- ☐ Design a training program for the staff involved to heighten information security awareness
- ☐ Set role-based access permissions on the shared folder
- ☐ The end user develops a PC macro program to compare sender and recipient file contents
- ☐ Shared folder operators sign an agreement to pledge not to commit fraudulent activities

Question 538

Key systems necessary for branch operations reside at corporate headquarters. Branch A is negotiating with a third party to provide disaster recovery facilities.

Which of the following contract terms would be the MOST significant concern?

- ☐ The hot site for the branch may have to be shared.
- ☐ Connectivity is not provided from the hot site to corporate headquarters.
- ☐ Penalty clauses for nonperformance are not included in contract.
- ☐ The right to audit the hot site is not provided in the contract.

Question 539

Which of the following information security metrics is the MOST difficult to quantify?

- ☐ Cost of security incidents prevented
- ☐ Percentage of controls mapped to industry frameworks
- ☐ Extent of employee security awareness
- ☐ Proportion of control costs to asset value

Question 540

What is the MOST important reason for conducting security awareness programs throughout an organization?

- ☐ Reducing the human risk
- ☐ Maintaining evidence of training records to ensure compliance
- ☐ Informing business units about the security strategy
- ☐ Training personnel in security incident response

Question 541

Which of the following security activities should be implemented in the change management process to identify key vulnerabilities introduced by changes?

- ☐ Business impact analysis (BIA)
- ☐ Penetration testing
- ☐ Audit and review
- ☐ Threat analysis

Question 542

Which of the following is characteristic of centralized information security management?

- ☐ More expensive to administer
- ☐ Better adherence to policies
- ☐ More aligned with business unit needs
- ☐ Faster turnaround of requests

Question 543

Which of the following BEST ensures timely and reliable access to services?

- ☐ Authenticity
- ☐ Recovery time objective
- ☐ Availability
- ☐ Nonrepudiation

Question 544

Which of the following is the MOST important reason for an organization to develop an information security governance program?

- ☐ Establishment of accountability
- ☐ Compliance with audit requirements
- ☐ Monitoring of security incidents
- ☐ Creation of tactical solutions

Question 545

The PRIMARY objective of a security steering group is to:

- ☐ ensure information security covers all business functions.
- ☐ ensure information security aligns with business goals.
- ☐ raise information security awareness across the organization.
- ☐ implement all decisions on security management across the organization.

Question 546

What is the MOST appropriate change management procedure for the handling of emergency program changes?

- ☐ Formal documentation does not need to be completed before the change
- ☐ Business management approval must be obtained prior to the change
- ☐ Documentation is completed with approval soon after the change
- ☐ All changes must follow the same process

Question 547

The FIRST step in an incident response plan is to:

- ☐ notify- the appropriate individuals.
- ☐ contain the effects of the incident to limit damage.
- ☐ develop response strategies for systematic attacks.
- ☐ validate the incident.

Question 548

Which of the following measures would be MOST effective against insider threats to confidential information?

- ☐ Role-based access control
- ☐ Audit trail monitoring
- ☐ Privacy policy
- ☐ Defense-in-depth

Question 549

When designing security controls, it is MOST important to:

- ☐ apply a risk-based approach.
- ☐ focus on preventive controls.
- ☐ evaluate the costs associated with the controls.
- ☐ apply controls to confidential information.

Question 550

Threat and vulnerability assessments are important PRIMARILY because they are:

- ☐ needed to estimate risk
- ☐ the basis for setting control objectives
- ☐ elements of the organization's security posture
- ☐ used to establish security investments

Question 551

Reevaluation of risk is MOST critical when there is:

- ☐ a change in security policy.
- ☐ resistance to the implementation of mitigating controls.
- ☐ a change in the threat landscape.
- ☐ a management request for updated security reports.

Question 552

Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

- ☐ Information security officer
- ☐ Security steering committee
- ☐ Data owner
- ☐ Data custodian

Question 553

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

- ☐ Automation of controls
- ☐ Documentation of control procedures
- ☐ Integration of assurance efforts
- ☐ Standardization of compliance requirements

Question 554

Business units within an organization are resistant to proposed changes to the information security program. Which of the following is the BEST way to address this issue?

- ☐ Implementing additional security awareness training
- ☐ Communicating critical risk assessment results to business unit managers
- ☐ Including business unit representation on the security steering committee
- ☐ Publishing updated information security policies

Question 555

Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

- ☐ Standards
- ☐ Guidelines
- ☐ Security metrics
- ☐ IT governance

Question 556

Which of the following would BEST detect malicious damage arising from an internal threat?

- ☐ Access control list
- ☐ Encryption
- ☐ Fraud awareness training
- ☐ Job rotation

Question 557

The criticality and sensitivity of information assets is determined on the basis of:

- ☐ threat assessment.
- ☐ vulnerability assessment.
- ☐ resource dependency assessment.
- ☐ impact assessment.

Question 558

Which of the following needs to be established between an IT service provider and its clients to the BEST enable adequate continuity of service in preparation for an outage?

- ☐ Data retention policies
- ☐ Server maintenance plans
- ☐ Recovery time objectives
- ☐ Reciprocal site agreement

Question 559

To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOST important item to include?

- ☐ Service level agreements (SLAs)
- ☐ Right to audit clause
- ☐ Intrusion detection system (IDS) services
- ☐ Spam filtering services

Question 560

An organization determines that an end-user has clicked on a malicious link. Which of the following would MOST effectively prevent similar situations from recurring?

- ☐ End-user training
- ☐ Virus protection
- ☐ End-user access control
- ☐ Updated security policies

Question 561

When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

- ☐ an adequate budget for the security program.
- ☐ recruitment of technical IT employees.
- ☐ periodic risk assessments.
- ☐ security awareness training for employees.

Question 562

Which of the following change management activities would be a clear indicator that normal operational procedures require examination? A high percentage of:

- ☐ similar change requests.
- ☐ change request postponements.
- ☐ canceled change requests.
- ☐ emergency change requests.

Question 563

Which of the following is the FIRST task when determining an organization's information security profile?

- ☐ Build an asset inventory
- ☐ List administrative privileges
- ☐ Establish security standards
- ☐ Complete a threat assessment

Question 564

Which of the following is MOST important to include in monthly information security reports to the board?

- ☐ Trend analysis of security metrics
- ☐ Threat intelligence
- ☐ Root cause analysis of security incidents
- ☐ Risk assessment results

Question 565

When building a corporate-wide business continuity plan, it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the BEST method to determine the priority of system recovery in the event of a disaster?

- ☐ Evaluating the cost associated with each system's outage
- ☐ Reviewing the business plans of each department
- ☐ Comparing the recovery point objectives (RPOs)
- ☐ Reviewing each system's key performance indicators (KPIs)

Question 566

Which of the following is MOST important for measuring the effectiveness of a security awareness program?

- ☐ Reduced number of security violation reports
- ☐ A quantitative evaluation to ensure user comprehension
- ☐ Increased interest in focus groups on security issues
- ☐ Increased number of security violation reports

Question 567

Which of the following is the MOST effective way to protect the authenticity of data in transit?

- ☐ Hash value
- ☐ Digital signature
- ☐ Public key
- ☐ Private key

Question 568

Which of the following would the BEST demonstrate the added value of an information security program?

- ☐ Security baselines
- ☐ A SWOT analysis
- ☐ A gap analysis
- ☐ A balanced scorecard

Question 569

Which of the following represents a PRIMARY area of interest when conducting a penetration test?

- ☐ Data mining
- ☐ Network mapping
- ☐ Intrusion Detection System (IDS)
- ☐ Customer data

Question 570

A CIO has asked the organization's information security manager to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

- ☐ To create formal requirements to meet projected security needs for the future
- ☐ To create and document a consistent progression of security capabilities
- ☐ To prioritize risks on a longer scale than the one-year plan
- ☐ To facilitate the continuous improvement of the IT organization

Question 571

Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

- ☐ Certificate-based authentication of web client
- ☐ Certificate-based authentication of web server
- ☐ Data confidentiality between client and web server
- ☐ Multiple encryption algorithms

Question 572

Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

- ☐ Utilize an intrusion detection system.
- ☐ Establish minimum security baselines.
- ☐ Implement vendor recommended settings.
- ☐ Perform periodic penetration testing.

Question 573

Which resource is the MOST effective in preventing physical access tailgating/piggybacking?

- ☐ Card key door locks
- ☐ Photo identification
- ☐ Awareness training
- ☐ Biometric scanners

Question 574

Which of the following is the MOST important consideration when selecting members for an information security steering committee?

- ☐ Cross-functional composition
- ☐ Information security expertise
- ☐ Tenure in the organization
- ☐ Business expertise

Question 575

What is the MOST important factor in the successful implementation of an enterprise wide information security program?

- ☐ Realistic budget estimates
- ☐ Security awareness
- ☐ Support of senior management
- ☐ Recalculation of the work factor

Question 576

An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

- ☐ Rewrite the application to conform to the upgraded operating system
- ☐ Compensate for not installing the patch with mitigating controls
- ☐ Alter the patch to allow the application to run in a privileged state
- ☐ Run the application on a test platform; tune production to allow patch and application

Question 577

An organization has to comply with recently published industry regulatory requirements — compliance that potentially has high implementation costs. What should the information security manager do FIRST?

- ☐ Implement a security committee.
- ☐ Perform a gap analysis.
- ☐ Implement compensating controls.
- ☐ Demand immediate compliance.

Question 578

An organization experienced a breach which was successfully contained and remediated. Based on industry regulations, the breach needs to be communicated externally. What should the information security manager do NEXT?

- ☐ Refer to the incident response plan.
- ☐ Send out a breach notification to all parties involved.
- ☐ Contact the board of directors.
- ☐ Invoke the corporate communications plan.

Question 579

Which of the following is the BEST way to demonstrate to senior management that organizational security practices comply with industry standards?

- ☐ Results of an independent assessment
- ☐ Up-to-date policy and procedures documentation
- ☐ A report on the maturity of controls
- ☐ Existence of an industry-accepted framework

Question 580

In assessing risk, it is MOST essential to:

- ☐ provide equal coverage for all asset types.
- ☐ use benchmarking data from similar organizations.
- ☐ consider both monetary value and likelihood of loss.
- ☐ focus primarily on threats and recent business losses.

Question 581

Which of the following guarantees that data in a file have not changed?

- ☐ Inspecting the modified date of the file
- ☐ Encrypting the file with symmetric encryption
- ☐ Using stringent access control to prevent unauthorized access
- ☐ Creating a hash of the file, then comparing the file hashes

Question 582

The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

- ☐ Laws and regulations of the country of origin may not be enforceable in the foreign country.
- ☐ A security breach notification might get delayed due to the time difference.
- ☐ Additional network intrusion detection sensors should be installed, resulting in an additional cost.
- ☐ The company could lose physical control over the server and be unable to monitor the physical security posture of the servers.

Question 583

The PRIMARY reason for using metrics to evaluate information security is to:

- ☐ identify security weaknesses.
- ☐ justify budgetary expenditures.
- ☐ enable steady improvement.
- ☐ raise awareness on security issues.

Question 584

Which of the following architectures for e-business BEST ensures high availability?

- ☐ Availability of an adjacent hot site and a standby server with mirrored copies of critical data
- ☐ Intelligent middleware to direct transactions from a downed system to an alternative
- ☐ A single point of entry allowing transactions to be received and processed quickly
- ☐ Automatic failover to the web site of another e-business that meets the user's needs

Question 585

Senior management commitment and support for information security can BEST be obtained through presentations that:

- ☐ use illustrative examples of successful attacks.
- ☐ explain the technical risks to the organization.
- ☐ evaluate the organization against best security practices.
- ☐ tie security risks to key business objectives.

Question 586

Which if the following would be the MOST important information to include in a business case for an information security project in a highly regulated industry?

- ☐ Compliance risk assessment
- ☐ Critical audit findings
- ☐ Industry comparison analysis
- ☐ Number of reported security incidents

Question 587

Which of the following will protect the confidentiality of data transmitted over the Internet?

- ☐ Message digests
- ☐ Network address translation
- ☐ Encrypting file system
- ☐ IPsec protocol

Question 588

The effectiveness of the information security process is reduced when an outsourcing organization:

- ☐ is responsible for information security governance activities
- ☐ receives additional revenue when security service levels are met
- ☐ incurs penalties for failure to meet security service-level agreements
- ☐ standardizes on a single access-control software product

Question 589

Which of the following is MOST important to the successful promotion of good security management practices?

- ☐ Security metrics
- ☐ Security baselines
- ☐ Management support
- ☐ Periodic training

Question 590

For an organization with a large and complex IT infrastructure, which of the following elements of a disaster recovery hot site service will require the closest monitoring?

- ☐ Employee access
- ☐ Audit rights
- ☐ Systems configurations
- ☐ Number of subscribers

Question 591

An organization's board of directors has learned of recent legislation requiring organizations within the industry to enact specific safeguards to protect confidential customer information. What actions should the board take next?

- ☐ Direct information security on what they need to do
- ☐ Research solutions to determine the proper solutions
- ☐ Require management to report on compliance
- ☐ Nothing; information security does not report to the board

Question 592

An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage cross training. Which type of authorization policy would BEST address this practice?

- ☐ Multilevel
- ☐ Role-based
- ☐ Discretionary
- ☐ Attribute-based

Question 593

A benefit of using a full disclosure (white box) approach as compared to a blind (black box) approach to penetration testing is that:

- ☐ it simulates the real-life situation of an external security attack.
- ☐ human intervention is not required for this type of test.
- ☐ less time is spent on reconnaissance and information gathering.
- ☐ critical infrastructure information is not revealed to the tester.

Question 594

An organization has been experiencing a number of network-based security attacks that all appear to originate internally. The BEST course of action is to:

- ☐ require the use of strong passwords.
- ☐ assign static IP addresses.
- ☐ implement centralized logging software.
- ☐ install an intrusion detection system (IDS).

Question 595

Which of the following would be of GREATEST assistance in determining whether to accept residual risk of a critical security system?

- ☐ Maximum tolerable outage (MTO)
- ☐ Cost-benefit analysis of mitigating controls
- ☐ Annual loss expectancy (ALE)
- ☐ Approved annual budget

Question 596

An executive's personal mobile device used for business purposes is reported lost. The information security manager should respond based on:

- ☐ mobile device configuration.
- ☐ asset management guidelines.
- ☐ the business impact analysis (BIA).
- ☐ incident classification.

Question 597

Labeling information according to its security classification:

- ☐ enhances the likelihood of people handling information securely.
- ☐ reduces the number and type of countermeasures required.
- ☐ reduces the need to identify baseline controls for each classification.
- ☐ affects the consequences if information is handled insecurely.

Question 598

The return on investment of information security can BEST be evaluated through which of the following?

- ☐ Support of business objectives
- ☐ Security metrics
- ☐ Security deliverables
- ☐ Process improvement models

Question 599

Organization A offers e-commerce services and uses secure transport protocol to protect Internet communication. To confirm communication with Organization A, which of the following would be the BEST for a client to verify?

- ☐ The certificate of the e-commerce server
- ☐ The browser's indication of SSL use
- ☐ The IP address of the e-commerce server
- ☐ The URL of the e-commerce server

Question 600

Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

- ☐ The activities being monitored deviate from what is considered normal.
- ☐ The information regarding monitored activities becomes stale.
- ☐ The pattern of normal behavior changes quickly and dramatically.
- ☐ The environment is complex.

Question 601

Which of the following is the MAIN benefit of performing an assessment of existing incident response processes?

- ☐ Identification of threats and vulnerabilities
- ☐ Prioritization of action plans
- ☐ Validation of current capabilities
- ☐ Benchmarking against industry peers

Question 602

What information is MOST helpful in demonstrating to senior management how information security governance aligns with business objectives?

- ☐ Updates on information security projects in development
- ☐ Drafts of proposed policy changes
- ☐ Metrics of key information security deliverables
- ☐ A list of monitored threats, risks, and exposures

Question 603

The PRIORITY action to be taken when a server is infected with a virus is to:

- ☐ isolate the infected server(s) from the network.
- ☐ identify all potential damage caused by the infection.
- ☐ ensure that the virus database files are current.
- ☐ establish security weaknesses in the firewall.

Question 604

A global organization has developed a strategy to share a customer information database between offices in two countries. In this situation, it is MOST important to ensure:

- ☐ data sharing complies with local laws and regulations at both locations.
- ☐ data is encrypted in transit and at rest.
- ☐ a nondisclosure agreement is signed.
- ☐ risk coverage is split between the two locations sharing data.

Question 605

Which of the following BEST facilitates the effective execution of an incident response plan?

- ☐ The response team is trained on the plan.
- ☐ The plan is based on risk assessment results.
- ☐ The incident response plan aligns with the IT disaster recovery plan.
- ☐ The plan is based on industry best practice.

Question 606

Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

- ☐ Virtual private network (VPN)
- ☐ Firewalls and routers
- ☐ Biometric authentication
- ☐ Two-factor authentication

Question 607

Minimum standards for securing the technical infrastructure should be defined in a security:

- ☐ strategy.
- ☐ guidelines.
- ☐ model.
- ☐ architecture.

Question 608

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized modification?

- ☐ Authenticity
- ☐ Availability
- ☐ Confidentiality
- ☐ Integrity

Question 609

Who is responsible for ensuring that information is classified?

- ☐ Senior management
- ☐ Security manager
- ☐ Data owner
- ☐ Custodian

Question 610

Before final acceptance of residual risk, what is the BEST way for an information security manager to address risk factors determined to be lower than acceptable risk levels?

- ☐ Evaluate whether an excessive level of control is being applied.
- ☐ Ask senior management to increase the acceptable risk levels.
- ☐ Implement more stringent countermeasures.
- ☐ Ask senior management to lower the acceptable risk levels.

Question 611

The PRIMARY reason for defining the information security roles and responsibilities of staff throughout an organization is to:

- ☐ reinforce the need for training
- ☐ increase corporate accountability
- ☐ comply with security policy
- ☐ enforce individual accountability

Question 612

Which of the following tasks should be performed once a disaster recovery plan has been developed?

- ☐ Analyze the business impact
- ☐ Define response team roles
- ☐ Develop the test plan
- ☐ Identify recovery time objectives

Question 613

An organization has recently experienced unauthorized device access to its network. To proactively manage the problem and mitigate this risk, the BEST preventive control would be to:

- ☐ keep an inventory of network and hardware addresses of all systems connected to the network.
- ☐ install a stateful inspection firewall to prevent unauthorized network traffic.
- ☐ implement network-level authentication and login to regulate access of devices to the network.
- ☐ deploy an automated asset inventory discovery tool to identify devices that access the network.

Question 614

Which of the following should be in place before a black box penetration test begins?

- ☐ IT management approval
- ☐ Proper communication and awareness training
- ☐ A clearly stated definition of scope
- ☐ An incident response plan

Question 615

Which of the following would be MOST useful to help senior management understand the status of information security compliance?

- ☐ Industry benchmarks
- ☐ Risk assessment results
- ☐ Business impact analysis (BIA) results
- ☐ Key performance indicators (KPIs)

Question 616

On a company's e-commerce web site, a good legal statement regarding data privacy should include:

- ☐ a statement regarding what the company will do with the information it collects.
- ☐ a disclaimer regarding the accuracy of information on its web site.
- ☐ technical information regarding how information is protected.
- ☐ a statement regarding where the information is being hosted.

Question 617

Which of the following is the MOST important consideration for designing an effective information security governance framework?

- ☐ Defined metrics
- ☐ Continuous audit cycle
- ☐ Security policy provisions
- ☐ Security controls automation

Question 618

What is the MOST cost-effective method of identifying new vendor vulnerabilities?

- ☐ External vulnerability reporting sources
- ☐ Periodic vulnerability assessments performed by consultants
- ☐ Intrusion prevention software
- ☐ honey pots located in the DMZ

Question 619

The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

- ☐ provide in-depth defense.
- ☐ separate test and production.
- ☐ permit traffic load balancing.
- ☐ prevent a denial-of-service attack.

Question 620

The MOST important reason to use a centralized mechanism to identify information security incidents is to:

- ☐ comply with corporate policies.
- ☐ prevent unauthorized changes to networks.
- ☐ threats across environments.
- ☐ detect potential fraud.

Question 621

When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

- ☐ Number of controls
- ☐ Cost of achieving control objectives
- ☐ Effectiveness of controls
- ☐ Test results of controls

Question 622

Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

- ☐ Provide security awareness training to the third-party provider's employees
- ☐ Conduct regular security reviews of the third-party provider
- ☐ Include security requirements in the service contract
- ☐ Request that the third-party provider comply with the organization's information security policy

Question 623

Which of the following is the MOST important objective of testing a security incident response plan?

- ☐ Confirm that systems are recovered in the proper order
- ☐ Verify the response assumptions are valid
- ☐ Ensure the thoroughness of the response plan
- ☐ Validate the business impact analysis

Question 624

A risk management program should reduce risk to:

- ☐ zero.
- ☐ an acceptable level.
- ☐ an acceptable percent of revenue.
- ☐ an acceptable probability of occurrence.

Question 625

The MOST complete business case for security solutions is one that.

- ☐ includes appropriate justification.
- ☐ explains the current risk profile.
- ☐ details regulatory requirements.
- ☐ identifies incidents and losses.

Question 626

Which of the following is the MAIN reason for performing risk assessment on a continuous basis'?

- ☐ Justification of the security budget must be continually made.
- ☐ New vulnerabilities are discovered every day.
- ☐ The risk environment is constantly changing.
- ☐ Management needs to be continually informed about emerging risks.

Question 627

After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

- ☐ increase its customer awareness efforts in those regions.
- ☐ implement monitoring techniques to detect and react to potential fraud.
- ☐ outsource credit card processing to a third party.
- ☐ make the customer liable for losses if they fail to follow the bank's advice.

Question 628

Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

- ☐ Configuration of firewalls
- ☐ Strength of encryption algorithms
- ☐ Authentication within application
- ☐ Safeguards over keys

Question 629

How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

- ☐ Give organization standards preference over local regulations
- ☐ Follow local regulations only
- ☐ Make the organization aware of those standards where local regulations causes conflicts
- ☐ Negotiate a local version of the organization standards

Question 630

A risk management program will be MOST effective when:

- ☐ risk appetite is sustained for a long period
- ☐ risk assessments are repeated periodically
- ☐ risk assessments are conducted by a third party
- ☐ business units are involved in risk assessments

Question 631

Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

- ☐ map the major threats to business objectives.
- ☐ review available sources of risk information.
- ☐ identify the value of the critical assets.
- ☐ determine the financial impact if threats materialize.

Question 632

A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The GREATEST weakness under this system architecture is that:

- ☐ users can gain direct access to the application ID and circumvent data controls.
- ☐ when multiple sessions with the same application ID collide, the database locks up.
- ☐ the database becomes unavailable if the password of the application ID expires.
- ☐ an incident involving unauthorized access to data cannot be tied to a specific user.

Question 633

The PRIMARY benefit of performing an information asset classification is to:

- ☐ link security requirements to business objectives.
- ☐ identify controls commensurate to risk.
- ☐ define access rights.
- ☐ establish ownership.

Question 634

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

- ☐ Warm
- ☐ Redundant
- ☐ Shared
- ☐ Mobile

Question 635

Which of the following are the MOST important individuals to include as members of an information security steering committee?

- ☐ Direct reports to the chief information officer
- ☐ IT management and key business process owners
- ☐ Cross-section of end users and IT professionals
- ☐ Internal audit and corporate legal departments

Question 636

What task should be performed once a security incident has been verified?

- ☐ Identify the incident.
- ☐ Contain the incident.
- ☐ Determine the root cause of the incident.
- ☐ Perform a vulnerability assessment.

Question 637

An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:

- ☐ document and report the root cause of the incidents for senior management.
- ☐ identify security program gaps or systemic weaknesses that need correction.
- ☐ prepare properly vetted notifications regarding the incidents to external parties.
- ☐ identify who should be held accountable for the security incidents.

Question 638

Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

- ☐ Encrypting first by receiver's private key and second by sender's public key
- ☐ Encrypting first by sender's private key and second by receiver's public key
- ☐ Encrypting first by sender's private key and second decrypting by sender's public key
- ☐ Encrypting first by sender's public key and second by receiver's private key

Question 639

A business unit intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should an information security manager take?

- ☐ Enforce the existing security standard
- ☐ Change the standard to permit the deployment
- ☐ Perform a risk analysis to quantify the risk
- ☐ Perform research to propose use of a better technology

Question 640

Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

- ☐ A bit-level copy of all hard drive data
- ☐ The last verified backup stored offsite
- ☐ Data from volatile memory
- ☐ Backup servers

Question 641

Which of the following is the MOST important factor in an organization's selection of a key risk indicator (KRI)?

- ☐ Return on investment
- ☐ Organizational culture
- ☐ Compliance requirements
- ☐ Criticality of information

Question 642

Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

- ☐ Delivery path tracing
- ☐ Reverse lookup translation
- ☐ Out-of-band channels
- ☐ Digital signatures

Question 643

Which of the following BEST indicates a successful risk management practice?

- ☐ Overall risk is quantified
- ☐ Inherent risk is eliminated
- ☐ Residual risk is minimized
- ☐ Control risk is tied to business units

Question 644

Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

- ☐ More uniformity in quality of service
- ☐ Better adherence to policies
- ☐ Better alignment to business unit needs
- ☐ More savings in total operating costs

Question 645

Logging is an example of which type of defense against systems compromise?

- ☐ Containment
- ☐ Detection
- ☐ Reaction
- ☐ Recovery

Question 646

What is the MOST effective access control method to prevent users from sharing files with unauthorized users?

- ☐ Mandatory
- ☐ Discretionary
- ☐ Walled garden
- ☐ Role-based

Question 647

When preventative controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager to perform?

- ☐ Assess vulnerabilities.
- ☐ Manage the impact.
- ☐ Evaluate potential threats.
- ☐ Identify unacceptable risk levels.

Question 648

Which of the following activities should take place FIRST when a security patch for Internet software is received from a vendor?

- ☐ The patch should be validated a hash algorithm.
- ☐ The patch should be applied to critical systems.
- ☐ The patch should be deployed quickly to systems that are vulnerable.
- ☐ The patch should be evaluated in a testing environment.

Question 649

Which of the following metrics is MOST appropriate for evaluating the incident notification process?

- ☐ Average total cost of downtime per reported incident
- ☐ Average number of incidents per reporting period
- ☐ Elapsed time between response and resolution
- ☐ Elapsed time between detection, reporting and response

Question 650

An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

- ☐ Review the procedures for granting access
- ☐ Establish procedures for granting emergency access
- ☐ Meet with data owners to understand business needs
- ☐ Redefine and implement proper access rights

Question 651

On which of the following should a firewall be placed?

- ☐ Web server
- ☐ Intrusion detection system (IDS) server
- ☐ Screened subnet
- ☐ Domain boundary

Question 652

A new regulation has been announced that requires mandatory reporting of security incidents that affect personal client information. Which of the following should be the information security manager's FIRST course of action?

- ☐ Review the current security policy.
- ☐ Inform senior management of the new regulation.
- ☐ Update the security incident management process.
- ☐ Determine impact to the business.

Question 653

A security awareness program should:

- ☐ present top management's perspective.
- ☐ address details on specific exploits.
- ☐ address specific groups and roles.
- ☐ promote security department procedures.

Question 654

During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:

- ☐ baseline security controls.
- ☐ cost-benefit analyses.
- ☐ benchmarking security metrics.
- ☐ security objectives.

Question 655

Which of the following would be the MOST significant security risk in a pharmaceutical institution?

- ☐ Compromised customer information
- ☐ Unavailability of online transactions
- ☐ Theft of security tokens
- ☐ Theft of a Research and Development laptop

Question 656

In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

- ☐ a strong authentication.
- ☐ IP antispoofing filtering.
- ☐ network encryption protocol.
- ☐ access lists of trusted devices.

Question 657

Which of the following is the BEST metric for evaluating the effectiveness of an intrusion detection mechanism?

- ☐ Number of attacks detected
- ☐ Number of successful attacks
- ☐ Ratio of false positives to false negatives
- ☐ Ratio of successful to unsuccessful attacks

Question 658

The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

- ☐ contribute cost-effective expertise not available internally.
- ☐ be made responsible for meeting the security program requirements.
- ☐ replace the dependence on internal resources.
- ☐ deliver more effectively on account of their knowledge.

Question 659

It is important to develop an information security baseline because it helps to define:

- ☐ critical information resources needing protection.
- ☐ a security policy for the entire organization.
- ☐ the minimum acceptable security to be implemented.
- ☐ required physical and logical access controls.

Question 660

The GREATEST benefit of choosing a private cloud over a public cloud would be:

- ☐ server protection.
- ☐ collection of data forensics.
- ☐ online service availability.
- ☐ containment of customer data.

Question 661

To ensure IT equipment meets organizational security standards, the MOST efficient approach is to:

- ☐ assess security during equipment deployment.
- ☐ ensure compliance during user acceptance testing.
- ☐ assess the risks of all new equipment.
- ☐ develop an approved equipment list.

Question 662

An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

- ☐ an audit of the service provider uncovers no significant weakness.
- ☐ the contract includes a nondisclosure agreement (NDA) to protect the organization's intellectual property.
- ☐ the contract should mandate that the service provider will comply with security policies.
- ☐ the third-party service provider conducts regular penetration testing.

Question 663

Which of the following would contribute MOST to employees' understanding of data handling responsibilities?

- ☐ Demonstrating support by senior management of the security program
- ☐ Requiring staff acknowledgement of security policies
- ☐ Labeling documents according to appropriate security classification
- ☐ Implementing a tailored security awareness training program

Question 664

Which of the following is an indicator of improvement in the ability to identify security risks?

- ☐ Increased number of reported security incidents.
- ☐ Decreased number of staff requiring information security training.
- ☐ Decreased number of information security risk assessments.
- ☐ Increased number of security audit issues resolved.

Question 665

While implementing information security governance an organization should FIRST:

- ☐ adopt security standards.
- ☐ determine security baselines.
- ☐ define the security strategy.
- ☐ establish security policies.

Question 666

A global organization processes and stores large volumes of personal data. Which of the following would be the MOST important attribute in creating a data access policy?

- ☐ Availability
- ☐ Integrity
- ☐ Reliability
- ☐ Confidentiality

Question 667

A post-incident review should be conducted by an incident management team to determine:

- ☐ relevant electronic evidence.
- ☐ lessons learned.
- ☐ hacker's identity.
- ☐ areas affected.

Question 668

To prevent computers on the corporate network from being used as part of a distributed denial of service attack, the information security manager should use:

- ☐ incoming traffic filtering
- ☐ outgoing traffic filtering
- ☐ IT security policy dissemination
- ☐ rate limiting

Question 669

Which of the following disaster recovery testing techniques is the MOST cost-effective way to determine the effectiveness of the plan?

- ☐ Preparedness tests
- ☐ Paper tests
- ☐ Full operational tests
- ☐ Actual service disruption

Question 670

The MAIN goal of an information security strategic plan is to:

- ☐ develop a risk assessment plan.
- ☐ develop a data protection plan.
- ☐ protect information assets and resources.
- ☐ establish security governance.

Question 671

Which of the following outsourced services has the GREATEST need for security monitoring?

- ☐ Enterprise infrastructure
- ☐ Application development
- ☐ Virtual private network (VPN) services
- ☐ Web site hosting

Question 672

When a new key business application goes into production, the PRIMARY reason to update relevant business impact analysis (BIA) and business continuity/disaster recovery plans is because:

- ☐ this is a requirement of the security policy.
- ☐ software licenses may expire in the future without warning.
- ☐ the asset inventory must be maintained.
- ☐ service level agreements may not otherwise be met.

Question 673

The business advantage of implementing authentication tokens is that they:

- ☐ provide nonrepudiation
- ☐ reduce overall cost
- ☐ improve access security
- ☐ reduce administrative workload

Question 674

At what stage of the applications development process would encryption key management initially be addressed?

- ☐ Requirements development
- ☐ Deployment
- ☐ Systems testing
- ☐ Code reviews

Question 675

Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

- ☐ Use security tokens for authentication
- ☐ Connect through an IPSec VPN
- ☐ Use https with a server-side certificate
- ☐ Enforce static media access control (MAC) addresses

Question 676

The management staff of an organization that does not have a dedicated security function decides to use its IT manager to perform a security review. The MAIN job requirement in this arrangement is that the IT manager

- ☐ report risks in other departments.
- ☐ obtain support from other departments.
- ☐ report significant security risks.
- ☐ have knowledge of security standards.

Question 677

Senior management has allocated funding to each of the organization's divisions to address information security vulnerabilities. The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?

- ☐ Areas of highest risk may not be adequately prioritized for treatment
- ☐ Redundant controls may be implemented across divisions
- ☐ Information security governance could be decentralized by division
- ☐ Return on investment may be inconsistently reported to senior management

Question 678

Which of the following MOST commonly falls within the scope of an information security governance steering committee?

- ☐ Interviewing candidates for information security specialist positions
- ☐ Developing content for security awareness programs
- ☐ Prioritizing information security initiatives
- ☐ Approving access to critical financial systems

Question 679

Which of the following groups would be in the BEST position to perform a risk analysis for a business?

- ☐ External auditors
- ☐ A peer group within a similar business
- ☐ Process owners
- ☐ A specialized management consultant

Question 680

Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

- ☐ Annual loss expectancy (ALE) of incidents
- ☐ Frequency of incidents
- ☐ Total cost of ownership (TCO)
- ☐ Approved budget for the project

Question 681

Which of the following should be performed FIRST in the aftermath of a denial-of-service attack?

- ☐ Restore servers from backup media stored offsite
- ☐ Conduct an assessment to determine system status
- ☐ Perform an impact analysis of the outage
- ☐ Isolate the screened subnet

Question 682

Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

- ☐ Patch management
- ☐ Change management
- ☐ Security metrics
- ☐ Version control

Question 683

Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

- ☐ Defining job roles
- ☐ Performing a risk assessment
- ☐ Identifying data owners
- ☐ Establishing data retention policies

Question 684

A digital signature using a public key infrastructure (PKI) will:

- ☐ not ensure the integrity of a message.
- ☐ rely on the extent to which the certificate authority (CA) is trusted.
- ☐ require two parties to the message exchange.
- ☐ provide a high level of confidentiality.

Question 685

The BEST metric for evaluating the effectiveness of a firewall is the:

- ☐ number of attacks blocked.
- ☐ number of packets dropped.
- ☐ average throughput rate.
- ☐ number of firewall rules.

Question 686

Which of the following is the BEST defense against distributed denial of service (DDoS) attacks?

- ☐ Multiple and redundant paths
- ☐ Well-configured routers and firewalls
- ☐ Regular patching
- ☐ Intruder-detection lockout

Question 687

Which of the following would be the MOST relevant factor when defining the information classification policy?

- ☐ Quantity of information
- ☐ Available IT infrastructure
- ☐ Benchmarking
- ☐ Requirements of data owners

Question 688

Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

- ☐ Programming
- ☐ Specification
- ☐ User testing
- ☐ Feasibility

Question 689

Which of the following is MOST effective in the strategic alignment of security initiatives?

- ☐ Key information security policies are updated on a regular basis.
- ☐ A security steering committee is set up within the IT department.
- ☐ Business leaders participate in information security decision making.
- ☐ Policies are created with input from business unit managers.

Question 690

Which of the following enables compliance with a nonrepudiation policy requirement for electronic transactions?

- ☐ Digital certificates
- ☐ Digital signatures
- ☐ Encrypted passwords
- ☐ One-time passwords

Question 691

An information security manager is reviewing the impact of a regulation on the organization's human resources system. The NEXT course of action should be to:

- ☐ perform a gap analysis of compliance requirements.
- ☐ assess the penalties for non-compliance.
- ☐ review the organization's most recent audit report.
- ☐ determine the cost of compliance.

Question 692

Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

- ☐ The right to conduct independent security reviews
- ☐ A legally binding data protection agreement
- ☐ Encryption between the organization and the provider
- ☐ A joint risk assessment of the system

Question 693

Which of the following is the BEST method to determine whether an information security program meets an organization's business objectives?

- ☐ Implement performance measures.
- ☐ Review against international security standards.
- ☐ Perform a business impact analysis (BIA).
- ☐ Conduct an annual enterprise-wide security evaluation.

Question 694

Information security awareness programs are MOST effective when they are:

- ☐ customized for each target audience.
- ☐ sponsored by senior management.
- ☐ reinforced by computer-based training.
- ☐ conducted at employee orientation

Question 695

Which of the following vulnerabilities presents the GREATEST risk of external hackers gaining access to the corporate network?

- ☐ Internal hosts running unnecessary services
- ☐ Inadequate logging
- ☐ Excessive administrative rights to an internal database
- ☐ Missing patches on a workstation

Question 696

Which of the following should be the MOST important criteria when defining data retention policies?

- ☐ Capacity requirements
- ☐ Audit findings
- ☐ Regulatory requirements
- ☐ Industry best practices

Question 697

Which of the following has the highest priority when defining an emergency response plan?

- ☐ Critical data
- ☐ Critical infrastructure
- ☐ Safety of personnel
- ☐ Vital records

Question 698

Which of the following would be MOST useful in a report to senior management for evaluating changes in the organization's information security risk position?

- ☐ Risk register
- ☐ Trend analysis
- ☐ Industry benchmarks
- ☐ Management action plan

Question 699

A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

- ☐ Access control policy
- ☐ Data classification policy
- ☐ Encryption standards
- ☐ Acceptable use policy

Question 700

When application-level security controlled by business process owners is found to be poorly managed, which of the following could BEST improve current practices?

- ☐ Centralizing security management
- ☐ Implementing sanctions for noncompliance
- ☐ Policy enforcement by IT management
- ☐ Periodic compliance reviews

Question 701

The MOST appropriate role for senior management in supporting information security is the:

- ☐ evaluation of vendors offering security products.
- ☐ assessment of risks to the organization.
- ☐ approval of policy statements and funding.
- ☐ monitoring adherence to regulatory requirements.

Question 702

Which of the following would BEST mitigate identified vulnerabilities in a timely manner?

- ☐ Continuous vulnerability monitoring tool
- ☐ Categorization of the vulnerabilities based on system's criticality
- ☐ Monitoring of key risk indicators (KRIs)
- ☐ Action plan with responsibilities and deadlines

Question 703

Which of the following defines the triggers within a business continuity plan (BCP)?

- ☐ Disaster recovery plan
- ☐ Needs of the organization
- ☐ Gap analysis
- ☐ Information security policy

Question 704

Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

- ☐ Conduct awareness sessions on intellectual property policy
- ☐ Require all employees to sign a nondisclosure agreement
- ☐ Promptly remove all access when an employee leaves the organization
- ☐ Restrict access to a need-to-know basis

Question 705

Which of the following individuals would be in the BEST position to sponsor the creation of an information security steering group?

- ☐ Information security manager
- ☐ Chief operating officer (COO)
- ☐ Internal auditor
- ☐ Legal counsel

Question 706

The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

- ☐ firewalls.
- ☐ bastion hosts.
- ☐ decoy files.
- ☐ screened subnets.

Question 707

An information security manager is recommending an investment in a new security initiative to address recently published threats. Which of the following would be MOST important to include in the business case?

- ☐ Business impact if threats materialize
- ☐ Availability of unused funds in the security budget
- ☐ Threat information from reputable sources
- ☐ Alignment of the new initiative with the approved business strategy

Question 708

Attackers who exploit cross-site scripting vulnerabilities take advantage of:

- ☐ a lack of proper input validation controls.
- ☐ weak authentication controls in the web application layer.
- ☐ flawed cryptographic secure sockets layer (SSL) implementations and short key lengths.
- ☐ implicit web application trust relationships.

Question 709

Risk management programs are designed to reduce risk to:

- ☐ a level that is too small to be measurable.
- ☐ the point at which the benefit exceeds the expense.
- ☐ a level that the organization is willing to accept.
- ☐ a rate of return that equals the current cost of capital.

Question 710

A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

- ☐ Enable access through a separate device that requires adequate authentication
- ☐ Implement manual procedures that require password change after each use
- ☐ Request the vendor to add multiple user IDs
- ☐ Analyze the logs to detect unauthorized access

Question 711

Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

- ☐ Incident response metrics
- ☐ Periodic auditing of the incident response process
- ☐ Action recording and review
- ☐ Post incident review

Question 712

Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

- ☐ To mitigate technical risks
- ☐ To have an independent certification of network security
- ☐ To receive an independent view of security exposures
- ☐ To identify a complete list of vulnerabilities

Question 713

Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?

- ☐ Senior management support
- ☐ Results of a cost-benefit analysis
- ☐ Results of a risk assessment
- ☐ Impact on the risk profile

Question 714

Which of the following BEST enables the deployment of consistent security throughout international branches within a multinational organization?

- ☐ Maturity of security processes
- ☐ Remediation of audit findings
- ☐ Decentralization of security governance
- ☐ Establishment of security governance

Question 715

When developing a tabletop test plan for incident response testing, the PRIMARY purpose of the scenario should be to:

- ☐ give the business a measure of the organization's overall readiness
- ☐ provide participants with situations to ensure understanding of their roles
- ☐ measure management engagement as part of an incident response team
- ☐ challenge the incident response team to solve the problem under pressure

Question 716

An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:

- ☐ source routing.
- ☐ broadcast propagation.
- ☐ unregistered ports.
- ☐ nonstandard protocols.

Question 717

Which of the following is the MOST likely outcome of a well-designed information security awareness course?

- ☐ Increased reporting of security incidents to the incident response function
- ☐ Decreased reporting of security incidents to the incident response function
- ☐ Decrease in the number of password resets
- ☐ Increase in the number of identified system vulnerabilities

Question 718

The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

- ☐ helps ensure that communications are secure.
- ☐ increases security between multi-tier systems.
- ☐ allows passwords to be changed less frequently.
- ☐ eliminates the need for secondary authentication.

Question 719

An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees flood the IT helpdesk with complaints of being unable to perform business functions on Internet sites. This is an example of:

- ☐ conflicting security controls with organizational needs.
- ☐ strong protection of information resources.
- ☐ implementing appropriate controls to reduce risk.
- ☐ proving information security's protective abilities.

Question 720

Which of the following would be MOST helpful to reduce the amount of time needed by an incident response team to determine appropriate actions?

- ☐ Providing annual awareness training regarding incident response for team members
- ☐ Defining incident severity levels during a business impact analysis (BIA)
- ☐ Validating the incident response plan against industry best practices
- ☐ Rehearsing incident response procedures, roles, and responsibilities

Question 721

When contracting with an outsourcer to provide security administration, the MOST important contractual element is the:

- ☐ right-to-terminate clause.
- ☐ limitations of liability.
- ☐ service level agreement (SLA).
- ☐ financial penalties clause.

Question 722

The BEST time to perform a penetration test is after:

- ☐ an attempted penetration has occurred.
- ☐ an audit has reported weaknesses in security controls.
- ☐ various infrastructure changes are made.
- ☐ a high turnover in systems staff.

Question 723

Segregation of duties is a security control PRIMARILY used to:

- ☐ establish dual check.
- ☐ establish hierarchy.
- ☐ limit malicious behavior.
- ☐ decentralize operations.

Question 724

The PRIMARY reason for creating a business case when proposing an information security project is to:

- ☐ establish the value of the project in relation to business objectives
- ☐ establish the value of the project with regard to regulatory compliance
- ☐ ensure relevant business parties are involved in the project
- ☐ ensure comprehensive security controls are identified

Question 725

A good privacy statement should include:

- ☐ notification of liability on accuracy of information.
- ☐ notification that information will be encrypted.
- ☐ what the company will do with information it collects.
- ☐ a description of the information classification process.

Question 726

The implementation of a capacity plan would prevent:

- ☐ file system overload arising from distributed denial-of-service attacks
- ☐ system downtime for scheduled security maintenance
- ☐ software failures arising from exploitation of buffer capacity vulnerabilities
- ☐ application failures arising from insufficient hardware resources

Question 727

The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

- ☐ the existence of messages is unknown.
- ☐ required key sizes are smaller.
- ☐ traffic cannot be sniffed.
- ☐ reliability of the data is higher in transit.

Question 728

Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

- ☐ Update platform-level security settings
- ☐ Conduct disaster recovery test exercises
- ☐ Approve access to critical financial systems
- ☐ Develop an information security strategy paper

Question 729

Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

- ☐ conduct a risk assessment and allow or disallow based on the outcome.
- ☐ recommend a risk assessment and implementation only if the residual risks are accepted.
- ☐ recommend against implementation because it violates the company's policies.
- ☐ recommend revision of current policy.

Question 730

The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

- ☐ Mitigating controls
- ☐ Visibility of impact
- ☐ Likelihood of occurrence
- ☐ Incident frequency

Question 731

A business partner of a factory has remote read-only access to material inventory to forecast future acquisition orders. An information security manager should PRIMARILY ensure that there is:

- ☐ an effective control over connectivity and continuity.
- ☐ a service level agreement (SLA) including code escrow.
- ☐ a business impact analysis (BIA).
- ☐ a third-party certification.

Question 732

Which of the following is MOST likely to be discretionary?

- ☐ Policies
- ☐ Procedures
- ☐ Guidelines
- ☐ Standards

Question 733

When aligning an organization's information security program with other risk and control activities, it is MOST important to:

- ☐ develop an information security governance framework.
- ☐ have information security management report to the chief risk officer.
- ☐ ensure adequate financial resources are available.
- ☐ integrate security within the system development life cycle.

Question 734

Which of the following is the MOST important requirement for setting up an information security infrastructure for a new system?

- ☐ Performing a business impact analysis (BIA)
- ☐ Considering personal information devices as part of the security policy
- ☐ Initiating IT security training and familiarization
- ☐ Basing the information security infrastructure on risk assessment

Question 735

In business-critical applications, user access should be approved by the:

- ☐ information security manager.
- ☐ data owner.
- ☐ data custodian.
- ☐ business management.

Question 736

Of the following, who should have PRIMARY responsibility for assessing the security risk associated with an outsourced cloud provider contract?

- ☐ Information security manager
- ☐ Compliance manager
- ☐ Chief information officer
- ☐ Service delivery manager

Question 737

Which of the following is the BEST indication of information security strategy alignment with the business?

- ☐ Number of business objectives directly supported by information security initiatives.
- ☐ Percentage of corporate budget allocated to information security initiatives.
- ☐ Number of business executives who have attended information security awareness sessions.
- ☐ Percentage of information security incidents resolved within defined service level agreements.

Question 738

An organization's marketing department wants to use an online collaboration service which is not in compliance with the information security policy. A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

- ☐ the information security manager
- ☐ business senior management
- ☐ the chief risk officer
- ☐ the compliance officer.

Question 739

Which of the following activities is used to determine the effect of a disruptive event?

- ☐ Maximum tolerable downtime assessment
- ☐ Recovery time objective (RTO) analysis
- ☐ Business impact analysis (BIA)
- ☐ Incident impact analysis

Question 740

Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

- ☐ Stress testing
- ☐ Patch management
- ☐ Change management
- ☐ Security baselines

Question 741

A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this decision is that:

- ☐ there are sufficient safeguards in place to prevent this risk from happening.
- ☐ the needed countermeasure is too complicated to deploy.
- ☐ the cost of countermeasure outweighs the value of the asset and potential loss.
- ☐ The likelihood of the risk occurring is unknown.

Question 742

Which of the following is MOST relevant for an information security manager to communicate to IT operations?

- ☐ The level of inherent risk
- ☐ Vulnerability assessments
- ☐ Threat assessments
- ☐ The level of exposure

Question 743

Which of the following roles would represent a conflict of interest for an information security manager?

- ☐ Evaluation of third parties requesting connectivity
- ☐ Assessment of the adequacy of disaster recovery plans
- ☐ Final approval of information security policies
- ☐ Monitoring adherence to physical security controls

Question 744

When implementing security architecture, an information security manager MUST ensure that security controls:

- ☐ form multiple barriers against threats.
- ☐ are transparent.
- ☐ are the least expensive.
- ☐ are communicated through security policies.

Question 745

The recovery point objective (RPO) is required in which of the following?

- ☐ Information security plan
- ☐ Incident response plan
- ☐ Business continuity plan
- ☐ Disaster recovery plan

Question 746

The PRIMARY goal of a security infrastructure design is the:

- ☐ reduction of security incidents.
- ☐ protection of corporate assets.
- ☐ elimination of risk exposures.
- ☐ optimization of IT resources.

Question 747

Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

- ☐ Cost to build a redundant processing facility and invocation
- ☐ Daily cost of losing critical systems and recovery time objectives (RTOs)
- ☐ Infrastructure complexity and system sensitivity
- ☐ Criticality results from the business impact analysis (BIA)

Question 748

After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

- ☐ Define security metrics
- ☐ Conduct a risk assessment
- ☐ Perform a gap analysis
- ☐ Procure security tools

Question 749

Who is ultimately responsible for the organization's information?

- ☐ Data custodian
- ☐ Chief information security officer (CISO)
- ☐ Board of directors
- ☐ Chief information officer (CIO)

Question 750

Data owners will determine what access and authorizations users will have by:

- ☐ delegating authority to data custodian.
- ☐ cloning existing user accounts.
- ☐ determining hierarchical preferences.
- ☐ mapping to business needs.

Question 751

Which of the following would be the BEST indicator that an organization is appropriately managing risk?

- ☐ The number of security incident events reported by staff has increased
- ☐ Risk assessment results are within tolerance
- ☐ A penetration test does not identify any high-risk system vulnerabilities
- ☐ The number of events reported from the intrusion detection system has declined

Question 752

An intrusion detection system should be placed:

- ☐ outside the firewall.
- ☐ on the firewall server.
- ☐ on a screened subnet.
- ☐ on the external router.

Question 753

Which of the following should be included in an annual information security budget that is submitted for management approval?

- ☐ A cost-benefit analysis of budgeted resources
- ☐ All of the resources that are recommended by the business
- ☐ Total cost of ownership (TCO)
- ☐ Baseline comparisons

Question 754

Good information security procedures should:

- ☐ define the allowable limits of behavior.
- ☐ underline the importance of security governance.
- ☐ describe security baselines for each platform.
- ☐ be updated frequently as new software is released.

Question 755

Which of the following is MOST important for an information security manager to regularly report to senior management?

- ☐ Results of penetration tests
- ☐ Audit reports
- ☐ Impact of unremediated risks
- ☐ Threat analysis reports

Question 756

A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

- ☐ Denial of service (DoS) attacks
- ☐ Traffic sniffing
- ☐ Virus infections
- ☐ IP address spoofing

Question 757

The MOST appropriate individual to determine the level of information security needed for a specific business application is the:

- ☐ system developer.
- ☐ information security manager.
- ☐ steering committee.
- ☐ system data owner.

Question 758

Which of the following is the PRIMARY objective of incident classification?

- ☐ Complying with regulatory requirements
- ☐ Increasing response efficiency
- ☐ Enabling incident reporting
- ☐ Reducing escalations to management

Question 759

Which two components PRIMARILY must be assessed in an effective risk analysis?

- ☐ Visibility and duration
- ☐ Likelihood and impact
- ☐ Probability and frequency
- ☐ Financial impact and duration

Question 760

Which of the following will BEST prevent an employee from using a USB drive to copy files from desktop computers?

- ☐ Restrict the available drive allocation on all PCs
- ☐ Disable universal serial bus (USB) ports on all desktop devices
- ☐ Conduct frequent awareness training with noncompliance penalties
- ☐ Establish strict access controls to sensitive information

Question 761

Which of the following is the MOST effective method of determining security priorities?

- ☐ Impact analysis
- ☐ Threat assessment
- ☐ Vulnerability assessment
- ☐ Gap analysis

Question 762

Which of the following should an information security manager perform FIRST when an organization's residual risk has increased?

- ☐ Implement security measures to reduce the risk.
- ☐ Communicate the information to senior management.
- ☐ Transfer the risk to third parties.
- ☐ Assess the business impact.

Question 763

The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

- ☐ hourly billing rate charged by the carrier.
- ☐ value of the data transmitted over the network.
- ☐ aggregate compensation of all affected business users.
- ☐ financial losses incurred by affected business units.

Question 764

Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

- ☐ Acceptable use policy
- ☐ Setting low mailbox limits
- ☐ User awareness training
- ☐ Taking disciplinary action

Question 765

An attacker was able to gain access to an organization's perimeter firewall and made changes to allow wider external access and to steal data. Which of the following would have BEST provided timely identification of this incident?

- ☐ Deploying a security information and event management system (SIEM)
- ☐ Deploying an intrusion prevention system (IPS)
- ☐ Implementing a data loss prevention (DLP) suite
- ☐ Conducting regular system administrator awareness training

Question 766

A multinational organization's information security manager has been advised that the city in which a contracted regional data center is located is experiencing civil unrest. The information security manager should FIRST:

- ☐ delete the organization's sensitive data at the provider's location
- ☐ engage another service provider at a safer location
- ☐ verify the provider's ability to protect the organization's data
- ☐ evaluate options to recover if the data center becomes unreachable

Question 767

When developing an information security program, what is the MOST useful source of information for determining available resources?

- ☐ Proficiency test
- ☐ Job descriptions
- ☐ Organization chart
- ☐ Skills inventory

Question 768

Which of the following is the MOST effective way to ensure information security policies are followed?

- ☐ Require sign-off on acceptable use policies.
- ☐ Require regular security awareness training.
- ☐ Provide detailed security procedures.
- ☐ Perform a gap analysis.

Question 769

When a significant security breach occurs, what should be reported FIRST to senior management?

- ☐ A summary of the security logs that illustrates the sequence of events
- ☐ An explanation of the incident and corrective action taken
- ☐ An analysis of the impact of similar attacks at other organizations
- ☐ A business case for implementing stronger logical access controls

Question 770

An organization's information security manager has been asked to hire a consultant to help assess the maturity level of the organization's information security management. The MOST important element of the request for proposal (RFP) is the:

- ☐ references from other organizations.
- ☐ past experience of the engagement team.
- ☐ sample deliverable.
- ☐ methodology used in the assessment.

Question 771

Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

- ☐ Symmetric cryptography
- ☐ Public key infrastructure (PKI)
- ☐ Message hashing
- ☐ Message authentication code

Question 772

Which of the following is a PRIMARY function of an incident response team?

- ☐ To provide a business impact assessment
- ☐ To provide effective incident mitigation
- ☐ To provide a single point of contact for critical incidents
- ☐ To provide a risk assessment for zero-day vulnerabilities

Question 773

Which of the following is the MOST effective way to address an organization's security concerns during contract negotiations with a third party?

- ☐ Ensure security is involved in the procurement process.
- ☐ Communicate security policy with the third-party vendor.
- ☐ Review the third-party contract with the organization's legal department.
- ☐ Conduct an information security audit on the third-party vendor.

Question 774

To achieve effective strategic alignment of security initiatives, it is important that:

- ☐ Steering committee leadership be selected by rotation.
- ☐ Inputs be obtained and consensus achieved between the major organizational units.
- ☐ The business strategy be updated periodically.
- ☐ Procedures and standards be approved by all departmental heads.

Question 775

In addition to business alignment and security ownership, which of the following is MOST critical for information security governance?

- ☐ Auditability of systems
- ☐ Compliance with policies
- ☐ Reporting of security metrics
- ☐ Executive sponsorship

Question 776

When developing an escalation process for an incident response plan, the information security manager should PRIMARILY consider the:

- ☐ media coverage.
- ☐ availability of technical resources.
- ☐ incident response team.
- ☐ affected stakeholders.

Question 777

The MOST important objective of monitoring key risk indicators (KRIs) related to information security is to:

- ☐ identify change in security exposures.
- ☐ reduce risk management costs.
- ☐ meet regulatory compliance requirements.
- ☐ minimize the loss from security incidents.

Question 778

Which of the following is the MOST appropriate method of ensuring password strength in a large organization?

- ☐ Attempt to reset several passwords to weaker values
- ☐ Install code to capture passwords for periodic audit
- ☐ Sample a subset of users and request their passwords for review
- ☐ Review general security settings on each platform

Question 779

After a server has been attacked, which of the following is the BEST course of action?

- ☐ Conduct a security audit
- ☐ Review vulnerability assessment
- ☐ Isolate the system
- ☐ Initiate incident response

Question 780

At what stage of the applications development process should the security department initially become involved?

- ☐ When requested
- ☐ At testing
- ☐ At programming
- ☐ At detail requirements

Question 781

An organization is planning to open a new office in another country. Sensitive data will be routinely sent between two offices. What should be the information security manager's FIRST course of action?

- ☐ Identify applicable regulatory requirements to establish security policies.
- ☐ Update privacy policies to include the other country's laws and regulations.
- ☐ Apply the current corporate security policies to the new office.
- ☐ Encrypt the data for transfer to the head office based on security manager approval.

Question 782

Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

- ☐ User ad hoc reporting is not logged
- ☐ Network traffic is through a single switch
- ☐ Operating system (OS) security patches have not been applied
- ☐ Database security defaults to ERP settings

Question 783

Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

- ☐ Baseline security standards
- ☐ System access violation logs
- ☐ Role-based access controls
- ☐ Exit routines

Question 784

Which of the following is the MOST important consideration when establishing an information security governance framework?

- ☐ Security steering committee meetings are held at least monthly.
- ☐ Members of the security steering committee are trained in information security.
- ☐ Business unit management acceptance is obtained.
- ☐ Executive management support is obtained.

Question 785

The chief information security officer (CISO) has developed an information security strategy, but is struggling to obtain senior management commitment for funds to implement the strategy.

Which of the following is the MOST likely reason?

- ☐ The strategy does not include a cost-benefit analysis.
- ☐ The CISO reports to the CIO.
- ☐ There was a lack of engagement with the business during development.
- ☐ The strategy does not comply with security standards.

Question 786

A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the BEST course of action to address the situation?

- ☐ Document the deficiencies in the risk register.
- ☐ Disconnect the legacy system from the rest of the network.
- ☐ Require that new systems that can meet the standards be implemented.
- ☐ Develop processes to compensate for the deficiencies.

Question 787

Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

- ☐ Intrusion detection system (IDS)
- ☐ IP address packet filtering
- ☐ Two-factor authentication
- ☐ Embedded digital signature

Question 788

Senior management has endorsed a comprehensive information security policy. Which of the following should the organization do NEXT?

- ☐ Promote awareness of the policy among employees.
- ☐ Seek policy buy-in from business stakeholders.
- ☐ Implement an authentication and authorization system.
- ☐ Identify relevant information security frameworks for adoption.

Question 789

To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:

- ☐ established guidelines
- ☐ criteria consistent with classification levels
- ☐ efficient technical processing considerations
- ☐ overall IT capacity and operational constraints

Question 790

Which of the following would be MOST helpful when justifying the funding required for a compensating control?

- ☐ Threat assessment
- ☐ Business impact analysis
- ☐ Business case
- ☐ Risk analysis

Question 791

Which metric is the BEST indicator that an update to an organization's information security awareness strategy is effective?

- ☐ A decrease in the number of incidents reported by staff
- ☐ A decrease in the number of email viruses detected
- ☐ An increase in the number of email viruses detected
- ☐ An increase in the number of incidents reported by staff

Question 792

It is MOST important that information security architecture be aligned with which of the following?

- ☐ Industry best practices
- ☐ Information technology plans
- ☐ Information security best practices
- ☐ Business objectives and goals

Question 793

What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

- ☐ Business impact analyses
- ☐ Security gap analyses
- ☐ System performance metrics
- ☐ Incident response processes

Question 794

The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

- ☐ results of exit interviews
- ☐ previous training sessions.
- ☐ examples of help desk requests.
- ☐ responses to security questionnaires.

Question 795

Access control to a sensitive intranet application by mobile users can BEST be implemented through:

- ☐ data encryption.
- ☐ digital signatures.
- ☐ strong passwords.
- ☐ two-factor authentication.

Question 796

When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:

- ☐ monitor for business changes
- ☐ review the residual risk level
- ☐ report compliance to management
- ☐ implement controls to mitigate the risk

Question 797

Which of the following would BEST prepare an information security manager for regulatory reviews?

- ☐ Assign an information security administrator as regulatory liaison
- ☐ Perform self-assessments using regulatory guidelines and reports
- ☐ Assess previous regulatory reports with process owners input
- ☐ Ensure all regulatory inquiries are sanctioned by the legal department

Question 798

Which of the following is the BEST course of action for the information security manager when residual risk is above the acceptable level of risk?

- ☐ Perform cost-benefit analysis
- ☐ Recommend additional controls
- ☐ Carry out risk assessment
- ☐ Defer to business management

Question 799

Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

- ☐ Require remote wipe capabilities for devices.
- ☐ Enforce passwords and data encryption on the devices.
- ☐ Conduct security awareness training.
- ☐ Review and update existing security policies.

Question 800

Which of the following threats is prevented by using token-based authentication?

- ☐ Password sniffing attack on the network
- ☐ Denial of service attack over the network
- ☐ Man-in-the-middle attack on the client
- ☐ Session eavesdropping attack on the network

Question 801

Which of the following is the MOST appropriate course of action when the risk occurrence rate is low but the impact is high?

- ☐ Risk transfer
- ☐ Risk acceptance
- ☐ Risk mitigation
- ☐ Risk avoidance

Question 802

An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

- ☐ A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
- ☐ Firewall policies are updated on the basis of changing requirements.
- ☐ inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
- ☐ The firewall is placed on top of the commercial operating system with all installation options.

Question 803

In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

- ☐ Applying patches
- ☐ Changing access rules
- ☐ Upgrading hardware
- ☐ Backing up files

Question 804

As an organization grows, exceptions to information security policies that were not originally specified may become necessary at a later date. In order to ensure effective management of business risks, exceptions to such policies should be:

- ☐ considered at the discretion of the information owner.
- ☐ approved by the next higher person in the organizational structure.
- ☐ formally managed within the information security framework.
- ☐ reviewed and approved by the security manager.

Question 805

During a security assessment, an information security manager finds a number of security patches were not installed on a server hosting a critical business application. The application owner did not approve the patch installation to avoid interrupting the application.

Which of the following should be the information security manager's FIRST course of action?

- ☐ Escalate the risk to senior management.
- ☐ Communicate the potential impact to the application owner.
- ☐ Report the risk to the information security steering committee.
- ☐ Determine mitigation options with IT management.

Question 806

Which of the following is MOST closely associated with a business continuity program?

- ☐ Confirming that detailed technical recovery plans exist
- ☐ Periodically testing network redundancy
- ☐ Updating the hot site equipment configuration every quarter
- ☐ Developing recovery time objectives (RTOs) for critical functions

Question 807

Which of the following is the BEST method for determining whether new risks exist in legacy applications?

- ☐ Regularly scheduled risk assessments
- ☐ Automated vulnerability scans
- ☐ Third-party penetration testing
- ☐ Frequent updates to the risk register

Question 808

An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

- ☐ Ethics
- ☐ Proportionality
- ☐ Integration
- ☐ Accountability

Question 809

Which of the following would provide the BEST justification for a new information security investment?

- ☐ Results of a comprehensive threat analysis.
- ☐ Projected reduction in risk.
- ☐ Senior management involvement in project prioritization.
- ☐ Defined key performance indicators (KPIs)

Question 810

Which of the following would be MOST effective in ensuring that information security is appropriately addressed in new systems?

- ☐ Internal audit signs off on security prior to implementation
- ☐ Information security staff perform compliance reviews before production begins
- ☐ Information security staff take responsibility for the design of system security
- ☐ Business requirements must include security objectives

Question 811

A large organization is in the process of developing its information security program that involves working with several complex organizational functions. Which of the following will BEST enable the successful implementation of this program?

- ☐ Security governance
- ☐ Security policy
- ☐ Security metrics
- ☐ Security guidelines

Question 812

The MOST important function of a risk management program is to:

- ☐ quantify overall risk.
- ☐ minimize residual risk.
- ☐ eliminate inherent risk.
- ☐ maximize the sum of all annualized loss expectancies (ALEs).

Question 813

The BEST way to establish a recovery time objective (RTO) that balances cost with a realistic recovery time frame is to:

- ☐ perform a business impact analysis.
- ☐ determine daily downtime cost.
- ☐ analyze cost metrics.
- ☐ conduct a risk assessment.

Question 814

When implementing effective security governance within the requirements of the company's security strategy, which of the following is the MOST important factor to consider?

- ☐ Preserving the confidentiality of sensitive data
- ☐ Establishing international security standards for data sharing
- ☐ Adhering to corporate privacy standards
- ☐ Establishing system manager responsibility for information security

Question 815

During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

- ☐ Feasibility
- ☐ Design
- ☐ Development
- ☐ Testing

Question 816

Which of the following is the MOST important factor when designing information security architecture?

- ☐ Technical platform interfaces
- ☐ Scalability of the network
- ☐ Development methodologies
- ☐ Stakeholder requirements

Question 817

An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?

- ☐ Nothing, since a risk assessment was completed during development.
- ☐ A vulnerability assessment should be conducted.
- ☐ A new risk assessment should be performed.
- ☐ The new vendor's SAS 70 type II report should be reviewed.

Question 818

Which of the following is the MOST important criterion for complete closure of a security incident?

- ☐ Level of potential impact
- ☐ Root-cause analysis and lessons learned
- ☐ Isolation and protection of affected resources
- ☐ Reporting to senior management

Question 819

Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

- ☐ Patch management
- ☐ Change management
- ☐ Security baselines
- ☐ Virus detection

Question 820

Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

- ☐ Never use open source tools
- ☐ Focus only on production servers
- ☐ Follow a linear process for attacks
- ☐ Do not interrupt production processes

Question 821

The MOST important characteristic of good security policies is that they:

- ☐ state expectations of IT management.
- ☐ state only one general security mandate.
- ☐ are aligned with organizational goals.
- ☐ govern the creation of procedures and guidelines.

Question 822

Which of the following BEST ensures that security risks will be reevaluated when modifications in application developments are made?

- ☐ A problem management process
- ☐ Background screening
- ☐ A change control process
- ☐ Business impact analysis (BIA)

Question 823

An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?

- ☐ Disable remote access
- ☐ Initiate a device reset
- ☐ Initiate incident response
- ☐ Conduct a risk assessment

Question 824

Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of integrity?

- ☐ Enforcing service level agreements
- ☐ Implementing a data classification schema
- ☐ Ensuring encryption for data in transit
- ☐ Utilizing a formal change management process

Question 825

When segregation of duties concerns exists between IT support staff and end users, what would be a suitable compensating control?

- ☐ Restricting physical access to computing equipment
- ☐ Reviewing transaction and application logs
- ☐ Performing background checks prior to hiring IT staff
- ☐ Locking user sessions after a specified period of inactivity

Question 826

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- ☐ Assimilation of the framework and intent of a written security policy by all appropriate parties
- ☐ Management support and approval for the implementation and maintenance of a security policy
- ☐ Enforcement of security rules by providing punitive actions for any violation of security rules
- ☐ Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Question 827

A data-hosting organization's data center houses servers, applications, and data for a large number of geographically dispersed customers. Which of the following strategies would be the BEST approach for developing a physical access control policy for the organization?

- ☐ Design single sign-on or federated access
- ☐ Conduct a risk assessment to determine security risks and mitigating controls
- ☐ Develop access control requirements for each system and application
- ☐ Review customers' security policies

Question 828

Which of the following should be PRIMARILY included in a security training program for business process owners?

- ☐ Impact of security risks
- ☐ Application vulnerabilities
- ☐ Application recovery time
- ☐ List of security incidents reported

Question 829

Which of the following is a PRIMARY responsibility of the information security governance function?

- ☐ Defining security strategies to support organizational programs
- ☐ Ensuring adequate support for solutions using emerging technologies
- ☐ Fostering a risk-aware culture to strengthen the information security program
- ☐ Advising senior management on optimal levels of risk appetite and tolerance

Question 830

When conducting a post-incident review, the GREATEST benefit of collecting mean time to resolution (MTTR) data is the ability to:

- ☐ reduce the costs of future preventive controls.
- ☐ provide metrics for reporting to senior management.
- ☐ learn of potential areas of improvement.
- ☐ verify compliance with the service level agreement (SLA).

Question 831

An organization experienced a data breach and followed its incident response plan. Later it was discovered that the plan was incomplete, omitting a requirement to report the incident to the relevant authorities. In addition to establishing an updated incident response plan, which of the following would be MOST helpful in preventing a similar occurrence?

- ☐ Attached reporting forms as an addendum to the incident response plan
- ☐ Management approval of the incident reporting process
- ☐ Ongoing evaluation of the incident response plan.
- ☐ Assignment of responsibility for communications.

Question 832

When facilitating the alignment of corporate governance and information security governance, which of the following is the MOST important role of an organization's security steering committee?

- ☐ Obtaining support for the integration from business owners
- ☐ Defining metrics to demonstrate alignment
- ☐ Obtaining approval for the information security budget
- ☐ Evaluating and reporting the degree of integration

Question 833

Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

- ☐ the parties to the agreement can perform.
- ☐ confidential data are not included in the agreement.
- ☐ appropriate controls are included.
- ☐ the right to audit is a requirement.

Question 834

Which of the following is done PRIMARILY to address the integrity of information?

- ☐ Assignment of appropriate control permissions
- ☐ Implementation of an Internet security application
- ☐ Implementation of a duplex server system
- ☐ Encryption of email

Question 835

When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

- ☐ Reboot the router connecting the DMZ to the firewall
- ☐ Power down all servers located on the DMZ segment
- ☐ Monitor the probe and isolate the affected segment
- ☐ Enable server trace logging on the affected segment

Question 836

Obtaining senior management support for establishing a warm site can BEST be accomplished by:

- ☐ establishing a periodic risk assessment.
- ☐ promoting regulatory requirements.
- ☐ developing a business case.
- ☐ developing effective metrics.

Question 837

Risk assessment is MOST effective when performed:

- ☐ at the beginning of security program development.
- ☐ on a continuous basis.
- ☐ while developing the business case for the security program.
- ☐ during the business change process.

Question 838

Which of the following would present the GREATEST risk to information security?

- ☐ Virus signature files updates are applied to all servers every day
- ☐ Security access logs are reviewed within five business days
- ☐ Critical patches are applied within 24 hours of their release
- ☐ Security incidents are investigated within five business days

Question 839

When an organization hires a new information security manager, which of the following goals should this individual pursue FIRST?

- ☐ Develop a security architecture
- ☐ Establish good communication with steering committee members
- ☐ Assemble an experienced staff
- ☐ Benchmark peer organizations

Question 840

Which of the following provides the MOST relevant information to determine the overall effectiveness of an information security program and underlying business processes?

- ☐ Balanced scorecard
- ☐ Cost-benefit analysis
- ☐ Industry benchmarks
- ☐ SWOT analysis

Question 841

During a review to approve a penetration test plan, which of the following should be an information security manager's PRIMARY concern?

- ☐ Penetration test team's deviation from scope
- ☐ Unauthorized access to administrative utilities
- ☐ False positive alarms to operations staff
- ☐ Impact on production systems

Question 842

Which of the following would be the BEST defense against sniffing?

- ☐ Password protect the files
- ☐ Implement a dynamic IP address scheme
- ☐ Encrypt the data being transmitted
- ☐ Set static mandatory access control (MAC) addresses

Question 843

Which of the following attacks is BEST mitigated by utilizing strong passwords?

- ☐ Man-in-the-middle attack
- ☐ Brute force attack
- ☐ Remote buffer overflow
- ☐ Root kit

Question 844

The PRIMARY purpose of performing an internal attack and penetration test as part of an incident response program is to identify:

- ☐ weaknesses in network and server security.
- ☐ ways to improve the incident response process.
- ☐ potential attack vectors on the network perimeter.
- ☐ the optimum response to internal hacker attacks.

Question 845

Which of the following is an advantage of a centralized information security organizational structure?

- ☐ It is easier to promote security awareness.
- ☐ It is easier to manage and control.
- ☐ It is more responsive to business unit needs.
- ☐ It provides a faster turnaround for security requests.

Question 846

Which of the following situations would be the MOST concern to a security manager?

- ☐ Audit logs are not enabled on a production server
- ☐ The logon ID for a terminated systems analyst still exists on the system
- ☐ The help desk has received numerous results of users receiving phishing e-mails
- ☐ A Trojan was found to be installed on a system administrator's laptop

Question 847

Which of the following actions should take place immediately after a security breach is reported to an information security manager?

- ☐ Confirm the incident
- ☐ Determine impact
- ☐ Notify affected stakeholders
- ☐ Isolate the incident

Question 848

An information security manager must understand the relationship between information security and business operations in order to:

- ☐ support organizational objectives.
- ☐ determine likely areas of noncompliance.
- ☐ assess the possible impacts of compromise.
- ☐ understand the threats to the business.

Question 849

Which of the following should be the MOST important consideration of business continuity management?

- ☐ Ensuring human safety
- ☐ Identifying critical business processes
- ☐ Ensuring the reliability of backup data
- ☐ Securing critical information assets

Question 850

Which of the following should be the PRIMARY consideration for an information security manager when designing security controls for a newly acquired business application?

- ☐ Known vulnerabilities in the application
- ☐ The IT security architecture framework
- ☐ Cost-benefit analysis of current controls
- ☐ Business processes supported by the application

Question 851

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the information security manager?

- ☐ Follow the outsourcer's response plan.
- ☐ Alert the appropriate law enforcement authorities.
- ☐ Refer to the organization's response plan.
- ☐ Notify the outsourcer of the privacy breach.

Question 852

Which of the following is the PRIMARY reason for executive management to be involved in establishing an enterprise's security management framework?

- ☐ To determine the desired state of enterprise security
- ☐ To establish the minimum level of controls needed
- ☐ To satisfy auditors' recommendations for enterprise security
- ☐ To ensure industry best practices for enterprise security are followed

Question 853

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain any effective information security program?

- ☐ Ensure information security is included in any change control efforts
- ☐ Merge the two information security programs to establish continuity
- ☐ Determine new factors that could influence the information security strategy
- ☐ Implement the current information security program in the acquired company

Question 854

An information security manager is reviewing the business case for a security project that is entering the development phase. It is determined that the estimated cost of the controls is now greater than the risk being mitigated.

The information security manager's BEST recommendation would be to:

- ☐ eliminate some of the controls from the project scope.
- ☐ discontinue the project to release funds for other efforts.
- ☐ pursue the project until the benefits cover the costs.
- ☐ slow the pace of the project to spread costs over a longer period.

Question 855

Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

- ☐ baseline.
- ☐ strategy.
- ☐ procedure.
- ☐ policy.

Question 856

Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

- ☐ Customer data stolen
- ☐ An electrical power outage
- ☐ A web site defaced by hackers
- ☐ Loss of the software development team

Question 857

A contract bid is digitally signed and electronically mailed. The PRIMARY advantage to using a digital signature is that:

- ☐ the bid and the signature can be copied from one document to another
- ☐ the bid cannot be forged even if the keys are compromised
- ☐ the signature can be authenticated even if no encryption is used
- ☐ any alteration of the bid will invalidate the signature

Question 858

In a business impact analysis, the value of an information system should be based on the overall cost:

- ☐ of recovery.
- ☐ to recreate.
- ☐ if unavailable.
- ☐ of emergency operations.

Question 859

An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

- ☐ Restrict account access to read only
- ☐ Log all usage of this account
- ☐ Suspend the account and activate only when needed
- ☐ Require that a change request be submitted for each download

Question 860

Which of the following is the BEST criterion to use when classifying assets?

- ☐ The market value of the assets
- ☐ Annual loss expectancy (ALE)
- ☐ Value of the assets relative to the organization
- ☐ Recovery time objective (RTO)

Question 861

Which of the following is the GREATEST risk of single sign-on?

- ☐ It is a single point of failure for an enterprise access control process.
- ☐ Password carelessness by one user may render the entire infrastructure vulnerable.
- ☐ Integration of single sign-on with the rest of the infrastructure is complicated.
- ☐ One administrator maintains the single sign-on solutions without segregation of duty.

Question 862

An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is MOST important to establish:

- ☐ automated reporting to stakeholders.
- ☐ a control self-assessment process.
- ☐ metrics for each milestone.
- ☐ a monitoring process for the security policy.

Question 863

Which of the following are seldom changed in response to technological changes?

- ☐ Standards
- ☐ Procedures
- ☐ Policies
- ☐ Guidelines

Question 864

A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

- ☐ System monitoring for traffic on network ports
- ☐ Security code reviews for the entire application
- ☐ Reverse engineering the application binaries
- ☐ Running the application from a high-privileged account on a test system

Question 865

To determine how a security breach occurred on the corporate network, a security manager looks at the logs of various devices. Which of the following BEST facilitates the correlation and review of these logs?

- ☐ Database server
- ☐ Domain name server (DNS)
- ☐ Time server
- ☐ Proxy server

Question 866

An audit has determined that employee use of personal mobile devices to access the company email system is resulting in confidential data leakage. The information security manager's FIRST course of action should be to:

- ☐ treat the situation as a security incident to determine appropriate response
- ☐ implement a data leakage prevention tool to stem further loss.
- ☐ isolate the mobile devices on the network for further investigation.
- ☐ treat the situation as a new risk and update the security risk register.

Question 867

Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed NEXT?

- ☐ Develop an implementation strategy.
- ☐ Schedule the target end date for implementation activities.
- ☐ Budget the total cost of implementation activities.
- ☐ Calculate the residual risk for each countermeasure.

Question 868

The MOST useful way to describe the objectives in the information security strategy is through:

- ☐ attributes and characteristics of the 'desired state.'
- ☐ overall control objectives of the security program.
- ☐ mapping the IT systems to key business processes.
- ☐ calculation of annual loss expectations.

Question 869

Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

- ☐ Budget allocation
- ☐ Technical skills of staff
- ☐ User acceptance
- ☐ Password requirements

Question 870

A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will own the process regarding the results and the assigned risk. Which of the following would be the BEST approach of the information security manager?

- ☐ Acceptance of the business manager's decision on the risk to the corporation
- ☐ Acceptance of the information security manager's decision on the risk to the corporation
- ☐ Review of the assessment with executive management for final input
- ☐ A new risk assessment and BIA are needed to resolve the disagreement

Question 871

Which of the following has the MOST direct impact on the usability of an organization's asset classification program?

- ☐ The granularity of classifications in the hierarchy
- ☐ The frequency of updates to the organization's risk register
- ☐ The business objectives of the organization
- ☐ The support of senior management for the classification scheme

Question 872

Attacks using multiple methods to spread should be classified:

- ☐ each time the exposure is experienced
- ☐ depending on the method used to spread
- ☐ at the highest potential level of business impact
- ☐ using multiple classifications for each impact

Question 873

Information security managers should use risk assessment techniques to:

- ☐ justify selection of risk mitigation strategies.
- ☐ maximize the return on investment (ROI).
- ☐ provide documentation for auditors and regulators.
- ☐ quantify risks that would otherwise be subjective.

Question 874

An information security manager has researched several options for handling ongoing security concerns and will be presenting these solutions to business managers. Which of the following will BEST enable business managers to make an informed decision?

- ☐ Business impact analysis
- ☐ Cost-benefit analysis
- ☐ Risk analysis
- ☐ Gap analysis

Question 875

Which of the following is the BEST method to securely transfer a message?

- ☐ Password-protected removable media
- ☐ Facsimile transmission in a secured room
- ☐ Using public key infrastructure (PKI) encryption
- ☐ Steganography

Question 876

Which of the following would be MOST effective in the strategic alignment of security initiatives?

- ☐ A security steering committee is set up within the IT department.
- ☐ Key information security policies are updated on a regular basis.
- ☐ Business leaders participate in information security decision making.
- ☐ Policies are created with input from business unit managers.

Question 877

During an information security audit, it was determined that IT staff did not follow the established standard when configuring and managing IT systems. Which of the following is the BEST way to prevent future occurrences?

- ☐ Updating configuration baselines to allow exceptions
- ☐ Conducting periodic vulnerability scanning
- ☐ Providing annual information security awareness training
- ☐ Implementing a strict change control process

Question 878

To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

- ☐ set their accounts to expire in six months or less.
- ☐ avoid granting system administration roles.
- ☐ ensure they successfully pass background checks.
- ☐ ensure their access is approved by the data owner.

Question 879

A risk profile support effective security decisions PRIMARILY because it:

- ☐ defines how the best mitigate future risks.
- ☐ identifies priorities for risk reduction.
- ☐ enables comparison with industry best practices.
- ☐ describes security threats.

Question 880

The MOST effective way to incorporate risk management practices into existing production systems is through:

- ☐ policy development.
- ☐ change management.
- ☐ awareness training.
- ☐ regular monitoring.

Question 881

An organization has learned of a security breach at another company that utilizes similar technology. The FIRST thing the information security manager should do is:

- ☐ assess the likelihood of incidents from the reported cause.
- ☐ discontinue the use of the vulnerable technology.
- ☐ report to senior management that the organization is not affected.
- ☐ remind staff that no similar security breaches have taken place.

Question 882

Which of the following would be the information security manager's BEST course of action to gain approval for investment in a technical control?

- ☐ Perform a cost-benefit analysis.
- ☐ Conduct a risk assessment.
- ☐ Calculate the exposure factor.
- ☐ Conduct a business impact analysis (BIA).

Question 883

Which of the following is the PRIMARY reason for implementing a risk management program?

- ☐ Allows the organization to eliminate risk
- ☐ Is a necessary part of management's due diligence
- ☐ Satisfies audit and regulatory requirements
- ☐ Assists in incrementing the return on investment (ROD)

Question 884

Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

- ☐ Adequate security policies and procedures
- ☐ Periodic compliance reviews
- ☐ Security steering committees
- ☐ Security awareness campaigns

Question 885

Which of the following would be MOST appropriate for collecting and preserving evidence?

- ☐ Encrypted hard drives
- ☐ Generic audit software
- ☐ Proven forensic processes
- ☐ Log correlation software

Question 886

When performing a risk assessment, the MOST important consideration is that:

- ☐ management supports risk mitigation efforts.
- ☐ annual loss expectations (ALEs) have been calculated for critical assets.
- ☐ assets have been identified and appropriately valued.
- ☐ attack motives, means and opportunities be understood.

Question 887

An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

- ☐ threat.
- ☐ loss.
- ☐ vulnerability.
- ☐ probability.

Question 888

Which of the following is MOST critical when creating an incident response plan?

- ☐ Identifying what constitutes an incident
- ☐ Identifying vulnerable data assets
- ☐ Aligning with the risk assessment process
- ☐ Documenting incident notification and escalation processes

Question 889

Information security projects should be prioritized on the basis of:

- ☐ time required for implementation.
- ☐ impact on the organization.
- ☐ total cost for implementation.
- ☐ mix of resources required.

Question 890

When training an incident response team, the advantage of using tabletop exercises is that they:

- ☐ provide the team with practical experience in responding to incidents
- ☐ ensure that the team can respond to any incident
- ☐ remove the need to involve senior managers in the response process
- ☐ enable the team to develop effective response interactions

Question 891

Effective IT governance is BEST ensured by:

- ☐ utilizing a bottom-up approach.
- ☐ management by the IT department.
- ☐ referring the matter to the organization's legal department.
- ☐ utilizing a top-down approach.

Question 892

When a security standard conflicts with a business objective, the situation should be resolved by:

- ☐ changing the security standard.
- ☐ changing the business objective.
- ☐ performing a risk analysis.
- ☐ authorizing a risk acceptance.

Question 893

When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

- ☐ Estimated productivity losses
- ☐ Possible scenarios with threats and impacts
- ☐ Value of information assets
- ☐ Vulnerability assessment

Question 894

Senior management has approved employees working off-site by using a virtual private network (VPN) connection. It is MOST important for the information security manager to periodically:

- ☐ perform a cost-benefit analysis
- ☐ review firewall configuration
- ☐ review the security policy
- ☐ perform a risk assessment

Question 895

Which of the following would BEST assist an IS manager in gaining strategic support from executive management?

- ☐ Annual report of security incidents within the organization
- ☐ Research on trends in global information security breaches
- ☐ Rating of the organization's security, based on international standards
- ☐ Risk analysis specific to the organization

Question 896

Which of the following is the MOST important reason to consider the role of the IT service desk when developing incident handling procedures?

- ☐ Service desk personnel have information on how to resolve common systems issues.
- ☐ The service desk provides a source for the identification of security incidents.
- ☐ The service desk provides information to prioritize systems recovery based on user.
- ☐ Untrained service desk personnel may be a cause of security incidents.

Question 897

It is MOST important for an information security manager to ensure that security risk assessments are performed:

- ☐ consistently throughout the enterprise
- ☐ during a root cause analysis
- ☐ as part of the security business case
- ☐ in response to the threat landscape

Question 898

When establishing escalation processes for an organization's computer security incident response team, the organization's procedures should:

- ☐ provide unrestricted communication channels to executive leadership to ensure direct access.
- ☐ require events to be escalated whenever possible to ensure that management is kept informed.
- ☐ recommend the same communication path for events to ensure consistency of communication.
- ☐ specify step-by-step escalation paths to ensure an appropriate chain of command.

Question 899

When developing a security architecture, which of the following steps should be executed FIRST?

- ☐ Developing security procedures
- ☐ Defining a security policy
- ☐ Specifying an access control methodology
- ☐ Defining roles and responsibilities

Question 900

When collecting evidence for forensic analysis, it is important to:

- ☐ ensure the assignment of qualified personnel.
- ☐ request the IT department do an image copy.
- ☐ disconnect from the network and isolate the affected devices.
- ☐ ensure law enforcement personnel are present before the forensic analysis commences.

Question 901

What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

- ☐ Risk assessment report
- ☐ Technical evaluation report
- ☐ Business case
- ☐ Budgetary requirements

Question 902

Which of the following will BEST enable an effective information asset classification process?

- ☐ Reviewing the recovery time objective (RTO) requirements of the asset
- ☐ Analyzing audit findings
- ☐ Including security requirements in the classification process
- ☐ Assigning ownership

Question 903

Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

- ☐ Interoffice a system-generated complex password with 30 days expiration
- ☐ Give a dummy password over the telephone set for immediate expiration
- ☐ Require no password but force the user to set their own in 10 days
- ☐ Set initial password equal to the user ID with expiration in 30 days

Question 904

Which of the following is the BEST way to determine if an information security program aligns with corporate governance?

- ☐ Evaluate funding for security initiatives
- ☐ Survey end users about corporate governance
- ☐ Review information security policies
- ☐ Review the balanced scorecard

Question 905

The BEST way to ensure that an external service provider complies with organizational security policies is to:

- ☐ Explicitly include the service provider in the security policies.
- ☐ Receive acknowledgment in writing stating the provider has read all policies.
- ☐ Cross-reference to policies in the service level agreement
- ☐ Perform periodic reviews of the service provider.

Question 906

Quantitative risk analysis is MOST appropriate when assessment data:

- ☐ include customer perceptions.
- ☐ contain percentage estimates.
- ☐ do not contain specific details.
- ☐ contain subjective information.

Question 907

Which of the following is the MOST important driver when developing an effective information security strategy?

- ☐ Information security standards
- ☐ Compliance requirements
- ☐ Benchmarking reports
- ☐ Security audit reports

Question 908

Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

- ☐ Authentication
- ☐ Hardening
- ☐ Encryption
- ☐ Nonrepudiation

Question 909

An e-commerce order fulfillment web server should generally be placed on which of the following?

- ☐ Internal network
- ☐ Demilitarized zone (DMZ)
- ☐ Database server
- ☐ Domain controller

Question 910

Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

- ☐ Business impact analysis (BIA)
- ☐ Risk assessment
- ☐ Vulnerability assessment
- ☐ Business process mapping

Question 911

Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

- ☐ determining the extent of property damage.
- ☐ preserving environmental conditions.
- ☐ ensuring orderly plan activation.
- ☐ reducing the extent of operational damage.

Question 912

Which of the following is the PRIMARY reason social media has become a popular target for attack?

- ☐ The prevalence of strong perimeter.
- ☐ The reduced effectiveness of access controls.
- ☐ The element of trust created by social media.
- ☐ The accessibility of social media from multiple locations.

Question 913

Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

- ☐ organizational risk.
- ☐ organization wide metrics.
- ☐ security needs.
- ☐ the responsibilities of organizational units.

Question 914

The FIRST step in developing an information security management program is to:

- ☐ identify business risks that affect the organization.
- ☐ clarify organizational purpose for creating the program.
- ☐ assign responsibility for the program.
- ☐ assess adequacy of controls to mitigate business risks.

Question 915

Authorization can BEST be accomplished by establishing:

- ☐ the ownership of the data.
- ☐ what users can do when they are granted system access.
- ☐ whether users are who they say they are.
- ☐ how users identify themselves to information systems.

Question 916

An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

- ☐ validate and sanitize client side inputs.
- ☐ harden the database listener component.
- ☐ normalize the database schema to the third normal form.
- ☐ ensure that the security patches are updated on operating systems.

Question 917

The MOST important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

- ☐ storage capacity and shelf life.
- ☐ regulatory and legal requirements.
- ☐ business strategy and direction.
- ☐ application systems and media.

Question 918

Which of the following is the MOST important component of information security governance?

- ☐ Approved Information security strategy
- ☐ Documented information security policies
- ☐ Comprehensive information security awareness program
- ☐ Appropriate information security metrics

Question 919

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

- ☐ Legal
- ☐ Information security
- ☐ Help desk
- ☐ Human resources

Question 920

A root kit was used to capture detailed accounts receivable information. To ensure admissibility of evidence from a legal standpoint, once the incident was identified and the server isolated, the next step should be to:

- ☐ document how the attack occurred.
- ☐ notify law enforcement.
- ☐ take an image copy of the media.
- ☐ close the accounts receivable system.

Question 921

Information security should be:

- ☐ focused on eliminating all risks.
- ☐ a balance between technical and business requirements.
- ☐ driven by regulatory requirements.
- ☐ defined by the board of directors.

Question 922

Which of the following are the MOST important criteria when selecting virus protection software?

- ☐ Product market share and annualized cost
- ☐ Ability to interface with intrusion detection system (IDS) software and firewalls
- ☐ Alert notifications and impact assessments for new viruses
- ☐ Ease of maintenance and frequency of updates

Question 923

Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?

- ☐ Risk acceptance by the business has been documented.
- ☐ Incident response and recovery plans are documented in simple language.
- ☐ Teams and individuals responsible for recovery have been identified.
- ☐ Copies of recovery and incident response plans are kept offsite.

Question 924

During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?

- ☐ Eradication
- ☐ Review
- ☐ Containment
- ☐ Identification

Question 925

Secure customer use of an e-commerce application can BEST be accomplished through:

- ☐ data encryption.
- ☐ digital signatures.
- ☐ strong passwords.
- ☐ two-factor authentication.

Question 926

Which of the following would BEST ensure the success of information security governance within an organization?

- ☐ Steering committees approve security projects
- ☐ Security policy training provided to all managers
- ☐ Security training available to all employees on the intranet
- ☐ Steering committees enforce compliance with laws and regulations

Question 927

Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

- ☐ Log all account usage and send it to their manager
- ☐ Establish predetermined automatic expiration dates
- ☐ Require managers to e-mail security when the user leaves
- ☐ Ensure each individual has signed a security acknowledgement

Question 928

What will have the HIGHEST impact on standard information security governance models?

- ☐ Number of employees
- ☐ Distance between physical locations
- ☐ Complexity of organizational structure
- ☐ Organizational budget

Question 929

To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

- ☐ create a separate account for the programmer as a power user.
- ☐ log all of the programmers' activity for review by supervisor.
- ☐ have the programmer sign a letter accepting full responsibility.
- ☐ perform regular audits of the application.

Question 930

Information security policy enforcement is the responsibility of the:

- ☐ security steering committee.
- ☐ chief information officer (CIO).
- ☐ chief information security officer (CISO).
- ☐ chief compliance officer (CCO).

Question 931

When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

- ☐ to a higher false reject rate (FRR).
- ☐ to a lower crossover error rate.
- ☐ to a higher false acceptance rate (FAR).
- ☐ exactly to the crossover error rate.

Question 932

Spoofing should be prevented because it may be used to:

- ☐ assemble information, track traffic, and identify network vulnerabilities.
- ☐ predict which way a program will branch when an option is presented.
- ☐ gain illegal entry to a secure system by faking the sender's address.
- ☐ capture information such as password traveling through the network.

Question 933

Which of the following is the MOST important item to include when developing web hosting agreements with third-party providers?

- ☐ Termination conditions
- ☐ Liability limits
- ☐ Service levels
- ☐ Privacy restrictions

Question 934

Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?

- ☐ Data ownership
- ☐ Data monitoring
- ☐ Data custodian
- ☐ Data encryption

Question 935

An organization is entering into an agreement with a new business partner to conduct customer mailings. What is the MOST important action that the information security manager needs to perform?

- ☐ A due diligence security review of the business partner's security controls
- ☐ Ensuring that the business partner has an effective business continuity program
- ☐ Ensuring that the third party is contractually obligated to all relevant security requirements
- ☐ Talking to other clients of the business partner to check references for performance

Question 936

Which of the following is the MOST important prerequisite to performing an information security risk assessment?

- ☐ Classifying assets
- ☐ Determining risk tolerance
- ☐ Reviewing the business impact analysis
- ☐ Assessing threats and vulnerabilities

Question 937

After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

- ☐ Senior management
- ☐ Business manager
- ☐ IT audit manager
- ☐ Information security officer (ISO)

Question 938

The BEST approach in managing a security incident involving a successful penetration should be to:

- ☐ allow business processes to continue during the response.
- ☐ allow the security team to assess the attack profile.
- ☐ permit the incident to continue to trace the source.
- ☐ examine the incident response process for deficiencies.

Question 939

Which of the following characteristics is MOST important to a bank in a high-value online financial transaction system?

- ☐ Identification
- ☐ Confidentiality
- ☐ Authentication
- ☐ Audit monitoring

Question 940

Which of the following is MOST important to verify when reviewing the effectiveness of response to an information security incident?

- ☐ Lessons learned have been implemented.
- ☐ Testing has been completed on time.
- ☐ Test results have been properly recorded.
- ☐ Metrics have been captured in a dashboard.

Question 941

Which of the following BEST indicates an effective vulnerability management program?

- ☐ Risks are managed within acceptable limits.
- ☐ Threats are identified accurately.
- ☐ Vulnerabilities are managed proactively.
- ☐ Vulnerabilities are reported in a timely manner.

Question 942

An organization has decided to implement a security information and event management (SIEM) system. It is MOST important for the organization to consider:

- ☐ industry best practices.
- ☐ data ownership.
- ☐ log sources.
- ☐ threat assessments.

Question 943

Which of the following is the MOST important to keep in mind when assessing the value of information?

- ☐ The potential financial loss
- ☐ The cost of recreating the information
- ☐ The cost of insurance coverage
- ☐ Regulatory requirement

Question 944

Which of the following should an information security manager establish FIRST to ensure security-related activities are adequately monitored?

- ☐ Internal reporting channels
- ☐ Accountability for security functions
- ☐ Scheduled security assessments
- ☐ Regular reviews of computer system logs

Question 945

Which of the following metrics would provide management with the MOST useful information about the progress of a security awareness program?

- ☐ Increased number of downloads of the organization's security policy
- ☐ Increased reported of security incidents
- ☐ Completion rate of user awareness training within each business unit
- ☐ Decreased number of security incidents

Question 946

Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

- ☐ corporate internal auditor.
- ☐ System developers/analysts.
- ☐ key business process owners.
- ☐ corporate legal counsel.

Question 947

An advantage of antivirus software schemes based on change detection is that they have:

- ☐ a chance of detecting current and future viral strains.
- ☐ a more flexible directory of viral signatures.
- ☐ to be updated less frequently than activity monitors.
- ☐ the highest probability of avoiding false alarms.

Question 948

What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

- ☐ Provide detailed instructions on how to carry out different types of tasks
- ☐ Ensure consistency of activities to provide a more stable environment
- ☐ Ensure compliance to security standards and regulatory requirements
- ☐ Ensure reusability to meet compliance to quality requirements

Question 949

In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

- ☐ Encryption
- ☐ Digital certificate
- ☐ Digital signature
- ☐ Hashing algorithm

Question 950

A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST:

- ☐ change the password policy to improve the customer experience
- ☐ research alternative secure methods of identity verification
- ☐ evaluate the impact of the customer's experience on business revenue
- ☐ recommend implementing two-factor authentication

Question 951

When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

- ☐ Business continuity plan
- ☐ Disaster recovery plan
- ☐ Incident response plan
- ☐ Vulnerability management plan

Question 952

What would be an information security manager's BEST recommendation upon learning that an existing contract with a third party does not clearly identify requirements for safeguarding the organization's critical data?

- ☐ Create an addendum to the existing contract.
- ☐ Cancel the outsourcing contract.
- ☐ Transfer the risk to the provider.
- ☐ Initiate an external audit of the provider's data center.

Question 953

A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following would be of MOST value?

- ☐ Examples of genuine incidents at similar organizations
- ☐ Statement of generally accepted best practices
- ☐ Associating realistic threats to corporate objectives
- ☐ Analysis of current technological exposures

Question 954

Which of the following is generally considered a fundamental component of an information security program?

- ☐ Role-based access control systems
- ☐ Automated access provisioning
- ☐ Security awareness training
- ☐ Intrusion prevention systems (IPSs)

Question 955

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

- ☐ security metrics
- ☐ service level agreements (SLAs)
- ☐ risk-reporting methodologies
- ☐ security requirements for the process being outsourced

Question 956

When developing an information security governance framework, which of the following should be the FIRST activity?

- ☐ Integrate security within the system's development life-cycle process.
- ☐ Align the information security program with the organization's other risk and control activities.
- ☐ Develop policies and procedures to support the framework.
- ☐ Develop response measures to detect and ensure the closure of security breaches.

Question 957

In the course of responding to an information security incident, the BEST way to treat evidence for possible legal action is defined by:

- ☐ international standards.
- ☐ local regulations.
- ☐ generally accepted best practices.
- ☐ organizational security policies.

Question 958

Which of the following is the MOST effective, positive method to promote security awareness?

- ☐ Competitions and rewards for compliance
- ☐ Lock-out after three incorrect password attempts
- ☐ Strict enforcement of password formats
- ☐ Disciplinary action for noncompliance

Question 959

When establishing an information security governance framework, it is MOST important for an information security manager to understand:

- ☐ the regulatory environment.
- ☐ information security best practices.
- ☐ the corporate culture.
- ☐ risk management techniques.

Question 960

Ensuring that activities performed by outsourcing providers comply with information security policies can BEST be accomplished through the use of:

- ☐ service level agreements.
- ☐ explicit contract language.
- ☐ local regulations.
- ☐ independent audits.

Question 961

When developing an information security strategy, the MOST important requirement is that:

- ☐ standards capture the intent of management.
- ☐ a schedule is developed to achieve objectives.
- ☐ the desired outcome is known.
- ☐ critical success factors (CSFs) are developed.

Question 962

Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

- ☐ Strategic business plan
- ☐ Upcoming financial results
- ☐ Customer personal information
- ☐ Previous financial results

Question 963

In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

- ☐ develop an operational plan for achieving compliance with the legislation.
- ☐ identify systems and processes that contain privacy components.
- ☐ restrict the collection of personal information until compliant.
- ☐ identify privacy legislation in other countries that may contain similar requirements.

Question 964

Which of the following is MOST important for a successful information security program?

- ☐ Adequate training on emerging security technologies
- ☐ Open communication with key process owners
- ☐ Adequate policies, standards and procedures
- ☐ Executive management commitment

Question 965

What should be an organization's MAIN concern when evaluating an Infrastructure as a Service (IaaS) cloud computing model for an e-Commerce application?

- ☐ Availability of provider's services
- ☐ Internal audit requirements
- ☐ Where the application resides
- ☐ Application ownership

Question 966

A user reports a stolen personal mobile device that stores sensitive corporate data. Which of the following will BEST minimize the risk of data exposure?

- ☐ Wipe the device remotely.
- ☐ Remove user's access to corporate data.
- ☐ Prevent the user from using personal mobile devices.
- ☐ Report the incident to the police.

Question 967

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

- ☐ relates information security policies and standards into business requirements
- ☐ relates the investment to the organization's strategic plan.
- ☐ realigns information security objectives to organizational strategy.
- ☐ articulates management's intent and information security directives in clear language.

Question 968

Which of the following would be a MAJOR consideration for an organization defining its business continuity plan (BCP) or disaster recovery program (DRP)?

- ☐ Setting up a backup site
- ☐ Maintaining redundant systems
- ☐ Aligning with recovery time objectives (RTOs)
- ☐ Data backup frequency

Question 969

Which of the following provides the GREATEST assurance that an organization allocates appropriate resources to respond to information security events?

- ☐ Threat analysis and intelligence reports
- ☐ Incident classification procedures
- ☐ Information security policies and standards
- ☐ An approved IT staffing plan

Question 970

Which of the following BEST describes the scope of risk analysis?

- ☐ Key financial systems
- ☐ Organizational activities
- ☐ Key systems and infrastructure
- ☐ Systems subject to regulatory compliance

Question 971

Which of the following be MOST effective in reducing the financial impact following a security breach leading to data disclosure?

- ☐ A business continuity plan
- ☐ Backup and recovery strategy
- ☐ A data loss prevention (DLP) solution
- ☐ An incident response plan

Question 972

A database was compromised by guessing the password for a shared administrative account and confidential customer information was stolen. The information security manager was able to detect this breach by analyzing which of the following?

- ☐ Invalid logon attempts
- ☐ Write access violations
- ☐ Concurrent logons
- ☐ Firewall logs

Question 973

Which of the following would be MOST important to include in a bring your own device (BYOD) policy with regard to lost or stolen devices? The need for employees to:

- ☐ initiate the company's incident reporting process.
- ☐ seek advice from the mobile service provider.
- ☐ notify local law enforcement.
- ☐ request a remote wipe of the device.

Question 974

A business impact analysis should be periodically executed PRIMARILY to:

- ☐ validate vulnerabilities on environmental changes.
- ☐ analyze the importance of assets.
- ☐ verify the effectiveness of controls.
- ☐ check compliance with regulations.

Question 975

Which of the following is the GREATEST benefit of integrating information security program requirements into vendor management?

- ☐ The ability to reduce risk in the supply chain
- ☐ The ability to meet industry compliance requirements
- ☐ The ability to define service level agreements (SLAs)
- ☐ The ability to improve vendor performance

Question 976

Which of the following is the MOST important reason to monitor information risk on a continuous basis?

- ☐ The risk profile can change over time.
- ☐ The effectiveness of controls can be verified.
- ☐ The cost of controls can be minimized.
- ☐ Risk assessment errors can be identified.

Question 977

To effectively manage an organization's information security risk, it is MOST important to:

- ☐ periodically identify and correct new systems vulnerabilities
- ☐ assign risk management responsibility to end users
- ☐ benchmark risk scenarios against peer organizations
- ☐ establish and communicate risk tolerance

Question 978

What is the GREATEST risk when there is an excessive number of firewall rules?

- ☐ One rule may override another rule in the chain and create a loophole
- ☐ Performance degradation of the whole network
- ☐ The firewall may not support the increasing number of rules due to limitations
- ☐ The firewall may show abnormal behavior and may crash or automatically shut down

Question 979

A security risk assessment exercise should be repeated at regular intervals because:

- ☐ business threats are constantly changing.
- ☐ omissions in earlier assessments can be addressed.
- ☐ repetitive assessments allow various methodologies.
- ☐ they help raise awareness on security in the business.

Question 980

Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

- ☐ Systems operation procedures are not enforced
- ☐ Change management procedures are poor
- ☐ Systems development is outsourced
- ☐ Systems capacity management is not performed

Question 981

Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

- ☐ SWOT analysis
- ☐ Waterfall chart
- ☐ Gap analysis
- ☐ Balanced scorecard

Question 982

What is the role of the information security manager in finalizing contract negotiations with service providers?

- ☐ To update security standards for the outsourced process
- ☐ To ensure that clauses for periodic audits are included
- ☐ To obtain a security standard certification from the provider
- ☐ To perform a risk analysis on the outsourcing process

Question 983

Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

- ☐ Ease of installation
- ☐ Product documentation
- ☐ Available support
- ☐ System overhead

Question 984

An information security manager is implementing a bring your own device (BYOD) program. Which of the following would BEST ensure that users adhere to the security standards?

- ☐ Monitor user activities on the network
- ☐ Publish the standards on the intranet landing page
- ☐ Establish an acceptable use policy
- ☐ Deploy a device management solution

Question 985

A security manager meeting the requirements for the international flow of personal data will need to ensure:

- ☐ a data processing agreement.
- ☐ a data protection registration.
- ☐ the agreement of the data subjects.
- ☐ subject access procedures.

Question 986

Which of the following BEST prepares a computer incident response team for a variety of information security scenarios?

- ☐ Tabletop exercises
- ☐ Forensics certification
- ☐ Penetration tests
- ☐ Disaster recovery drills

Question 987

Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

- ☐ Tree diagrams
- ☐ Venn diagrams
- ☐ Heat charts
- ☐ Bar charts

Question 988

The BEST way to report to the board on the effectiveness of the information security program is to present:

- ☐ a dashboard illustrating key performance metrics.
- ☐ peer-group industry benchmarks.
- ☐ a summary of the most recent audit findings.
- ☐ a report of cost savings from process improvements.

Question 989

The PRIMARY purpose of using risk analysis within a security program is to:

- ☐ justify the security expenditure.
- ☐ help businesses prioritize the assets to be protected.
- ☐ inform executive management of residual risk value.
- ☐ assess exposures and plan remediation.

Question 990

For an organization with operations in different parts of the world, the BEST approach for ensuring that security policies do not conflict with local laws and regulations is to:

- ☐ refer to an external global standard to avoid any regional conflict
- ☐ make policies at a sufficiently high level, so they are globally applicable
- ☐ adopt uniform policies
- ☐ establish a hierarchy of global and local policies

Question 991

Simple Network Management Protocol v2 (SNMP v2) is used frequently to monitor networks. Which of the following vulnerabilities does it always introduce?

- ☐ Remote buffer overflow
- ☐ Cross site scripting
- ☐ Clear text authentication
- ☐ Man-in-the-middle attack

Question 992

The PRIMARY purpose of installing an intrusion detection system (IDS) is to identify:

- ☐ weaknesses in network security.
- ☐ patterns of suspicious access.
- ☐ how an attack was launched on the network.
- ☐ potential attacks on the internal network.

Question 993

A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

- ☐ confirm the incident.
- ☐ notify senior management.
- ☐ start containment.
- ☐ notify law enforcement.

Question 994

Which of the following risks is represented in the risk appetite of an organization?

- ☐ Control
- ☐ Inherent
- ☐ Residual
- ☐ Audit

Question 995

Which of the following is MOST helpful to maintain cohesiveness within an organization's information security resource?

- ☐ Information security architecture
- ☐ Security gap analysis
- ☐ Business impact analysis
- ☐ Information security steering committee

Question 996

The PRIMARY reason for involving information security at each stage in the systems development life cycle (SDLC) is to identify the security implications and potential solutions required for:

- ☐ identifying vulnerabilities in the system.
- ☐ sustaining the organization's security posture.
- ☐ the existing systems that will be affected.
- ☐ complying with segregation of duties.

Question 997

A risk profile supports effective security decisions PRIMARILY because it:

- ☐ defines how to best mitigate future risks.
- ☐ identifies priorities for risk reduction.
- ☐ enables comparison with industry best practices.
- ☐ describes security threats.

Question 998

Which of the following is the MOST effective data loss control when connecting a personally owned mobile device to the corporate email system?

- ☐ Email must be stored in an encrypted format on the mobile device.
- ☐ Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
- ☐ A senior manager must approve each connection.
- ☐ Users must agree to allow the mobile device to be wiped if it is lost.

Question 999

A critical component of a continuous improvement program for information security is:

- ☐ measuring processes and providing feedback.
- ☐ developing a service level agreement (SLA) for security.
- ☐ tying corporate security standards to a recognized international standard.
- ☐ ensuring regulatory compliance.

Question 1000

What is the MOST cost-effective means of improving security awareness of staff personnel?

- ☐ Employee monetary incentives
- ☐ User education and training
- ☐ A zero-tolerance security policy
- ☐ Reporting of security infractions

Question 1001

Which of the following would BEST help to ensure the alignment between information security and business functions?

- ☐ Establishing an information security governance committee
- ☐ Developing information security policies
- ☐ Providing funding for information security efforts
- ☐ Establishing a security awareness program

Question 1002

Which of the following is a step in establishing a security policy?

- ☐ Developing platform-level security baselines
- ☐ Creating a RACI matrix
- ☐ Implementing a process for developing and maintaining the policy
- ☐ Developing configuration parameters for the network

Question 1003

The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

- ☐ escalate issues to an external third party for resolution.
- ☐ ensure that senior management provides authority for security to address the issues.
- ☐ insist that managers or units not in agreement with the security solution accept the risk.
- ☐ refer the issues to senior management along with any security recommendations.

Question 1004

Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

- ☐ Request a list of the software to be used
- ☐ Provide clear directions to IT staff
- ☐ Monitor intrusion detection system (IDS) and firewall logs closely
- ☐ Establish clear rules of engagement

Question 1005

Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

- ☐ Gap analysis
- ☐ Regression analysis
- ☐ Risk analysis
- ☐ Business impact analysis

Question 1006

An information security manager is asked to provide evidence that the organization is fulfilling its legal obligation to protect personally identifiable information (PII).

Which of the following would be MOST helpful for this purpose?

- ☐ Metrics related to program effectiveness
- ☐ Written policies and standards
- ☐ Privacy awareness training
- ☐ Risk assessments of privacy-related applications

Question 1007

An organization wants to enable digital forensics for a business-critical application. Which of the following will BEST help to support this objective?

- ☐ Install biometric access control.
- ☐ Develop an incident response plan.
- ☐ Define data retention criteria.
- ☐ Enable activity logging.

Question 1008

Investment in security technology and processes should be based on:

- ☐ clear alignment with the goals and objectives of the organization.
- ☐ success cases that have been experienced in previous projects.
- ☐ best business practices.
- ☐ safeguards that are inherent in existing technology.

Question 1009

The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

- ☐ periodically testing the incident response plans.
- ☐ regularly testing the intrusion detection system (IDS).
- ☐ establishing mandatory training of all personnel.
- ☐ periodically reviewing incident response procedures.

Question 1010

With limited resources in the information security department, which of the following is the BEST approach for managing security risk?

- ☐ Implement technical solutions to automate security management activities.
- ☐ Prioritize security activities and report to management.
- ☐ Hire additional information security staff.
- ☐ Engage a third-party company to provide security support.

Question 1011

To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:

- ☐ noncompliance issues are reported to senior management
- ☐ information security management understands business performance issues
- ☐ the security policy is changed to accommodate IT performance pressure
- ☐ senior management provides guidance and dispute resolution

Question 1012

When reviewing the security controls of an application service provider, an information security manager discovers the provider's change management controls are insufficient. Changes to the provided application often occur spontaneously with no notification to clients. Which of the following would BEST facilitate a decision to continue or discontinue services with this provider?

- ☐ Comparing the client organization's risk appetite to the disaster recovery plan of the service provider.
- ☐ Comparing the client organization's risk appetite to the criticality of the supplied application.
- ☐ Comparing the client organization's risk appetite to the frequency of application downtimes.
- ☐ Comparing the client organization's risk appetite to the vendor's change control policy.

Question 1013

An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done NEXT to address this concern?

- ☐ Conduct a risk analysis
- ☐ Escalate to the chief risk officer
- ☐ Conduct a vulnerability analysis
- ☐ Determine compensating controls

Question 1014

When an organization is implementing an information security governance program, its board of directors should be responsible for:

- ☐ drafting information security policies.
- ☐ reviewing training and awareness programs.
- ☐ setting the strategic direction of the program.
- ☐ auditing for compliance.

Question 1015

After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?

- ☐ Risk heat map
- ☐ Recent audit results
- ☐ Balanced scorecard
- ☐ Gap analysis

Question 1016

Which of the following reduces the potential impact of social engineering attacks?

- ☐ Compliance with regulatory requirements
- ☐ Promoting ethical understanding
- ☐ Security awareness programs
- ☐ Effective performance incentives

Question 1017

What is the MOST important success factor in launching a corporate information security awareness program?

- ☐ Adequate budgetary support
- ☐ Centralized program management
- ☐ Top-down approach
- ☐ Experience of the awareness trainers

Question 1018

What is the BEST defense against a Structured Query Language (SQL) injection attack?

- ☐ Regularly updated signature files
- ☐ A properly configured firewall
- ☐ An intrusion detection system
- ☐ Strict controls on input fields

Question 1019

An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

- ☐ Inform senior management.
- ☐ Determine the extent of the compromise.
- ☐ Report the incident to the authorities.
- ☐ Communicate with the affected customers.

Question 1020

Which item would be the BEST to include in the information security awareness training program for new general staff employees?

- ☐ Review of various security models
- ☐ Discussion of how to construct strong passwords
- ☐ Review of roles that have privileged access
- ☐ Discussion of vulnerability assessment results

Question 1021

Which of the following should be an information security manager's MOST important concern to ensure admissibility of information security evidence from cyber crimes?

- ☐ Chain of custody
- ☐ Tools used for evidence analysis
- ☐ Forensics contractors
- ☐ Efficiency of the forensics team

Question 1022

Which of the following is the MOST important risk associated with middleware in a client-server environment?

- ☐ Server patching may be prevented
- ☐ System backups may be incomplete
- ☐ System integrity may be affected
- ☐ End-user sessions may be hijacked

Question 1023

Which of the following is the MOST important information to include in an information security standard?

- ☐ Creation date
- ☐ Author name
- ☐ Initial draft approval date
- ☐ Last review date

Question 1024

Which of the following should be the FIRST step in developing an information security plan?

- ☐ Perform a technical vulnerabilities assessment
- ☐ Analyze the current business strategy
- ☐ Perform a business impact analysis
- ☐ Assess the current levels of security awareness

Question 1025

The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

- ☐ regulatory' requirements.
- ☐ business requirements.
- ☐ financial value.
- ☐ IT resource availability.

Question 1026

Which of the following is the PRIMARY benefit of using agentless endpoint security solutions?

- ☐ Decreased network bandwidth usage
- ☐ Decreased administration
- ☐ Increased resiliency
- ☐ More comprehensive information results

Question 1027

The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

- ☐ Secure Sockets Layer (SSL).
- ☐ Secure Shell (SSH).
- ☐ IP Security (IPSec).
- ☐ Secure/Multipurpose Internet Mail Extensions (S/MIME).

Question 1028

Of the following, whose input is of GREATEST importance in the development of an information security strategy?

- ☐ End users
- ☐ Corporate auditors
- ☐ Process owners
- ☐ Security architects

Question 1029

A desktop computer that was involved in a computer security incident should be secured as evidence by:

- ☐ disconnecting the computer from all power sources.
- ☐ disabling all local user accounts except for one administrator.
- ☐ encrypting local files and uploading exact copies to a secure server.
- ☐ copying all files using the operating system (OS) to write-once media.

Question 1030

The MOST important factor in ensuring the success of an information security program is effective:

- ☐ communication of information security requirements to all users in the organization.
- ☐ formulation of policies and procedures for information security.
- ☐ alignment with organizational goals and objectives.
- ☐ monitoring compliance with information security policies and procedures.

Question 1031

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the MOST useful information for planning purposes?

- ☐ Results from a gap analysis
- ☐ Results from a business impact analysis
- ☐ Deadlines and penalties for noncompliance
- ☐ An inventory of security controls currently in place

Question 1032

The BEST way to encourage good security practices is to:

- ☐ schedule periodic compliance audits.
- ☐ discipline those who fail to comply with the security policy.
- ☐ recognize appropriate security behavior by individuals.
- ☐ publish the information security policy.

Question 1033

The PRIMARY focus of a training curriculum for members of an incident response team should be:

- ☐ specific role training
- ☐ external corporate communication
- ☐ security awareness
- ☐ technology training

Question 1034

For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

- ☐ Biometrics
- ☐ Symmetric encryption keys
- ☐ Secure Sockets Layer (SSL)-based authentication
- ☐ Two-factor authentication

Question 1035

A PRIMARY purpose of creating security policies is to:

- ☐ implement management's governance strategy.
- ☐ establish the way security tasks should be executed.
- ☐ communicate management's security expectations.
- ☐ define allowable security boundaries.

Question 1036

An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

- ☐ broken authentication.
- ☐ unvalidated input.
- ☐ cross-site scripting.
- ☐ structured query language (SQL) injection.

Question 1037

When creating a forensic image of a hard drive, which of the following should be the FIRST step?

- ☐ Identify a recognized forensics software tool to create the image.
- ☐ Establish a chain of custody log.
- ☐ Connect the hard drive to a write blocker.
- ☐ Generate a cryptographic hash of the hard drive contents.

Question 1038

When customer data has been compromised, an organization should contact law enforcement authorities:

- ☐ if the attack comes from an international source.
- ☐ when directed by the information security manager.
- ☐ if there is potential impact to the organization.
- ☐ in accordance with the corporate communication policy.

Question 1039

What is the BEST technique to determine which security controls to implement with a limited budget?

- ☐ Risk analysis
- ☐ Annualized loss expectancy (ALE) calculations
- ☐ Cost-benefit analysis
- ☐ Impact analysis

Question 1040

Managing the life cycle of a digital certificate is a role of a(n):

- ☐ system administrator.
- ☐ security administrator.
- ☐ system developer.
- ☐ independent trusted source.

Question 1041

Ensuring that activities performed by outsourcing providers comply with information security policies can BEST be accomplished through the use of:

- ☐ service level agreements.
- ☐ independent audits.
- ☐ explicit contract language.
- ☐ local regulations.

Question 1042

An organization to integrate information security into its human resource management processes. Which of the following should be the FIRST step?

- ☐ Evaluate the cost of information security integration
- ☐ Assess the business objectives of the processes
- ☐ Identify information security risk associated with the processes
- ☐ Benchmark the processes with best practice to identify gaps

Question 1043

Utilizing external resources for highly technical information security tasks allows an information security manager to:

- ☐ distribute technology risk.
- ☐ leverage limited resources.
- ☐ outsource responsibility.
- ☐ transfer business risk.

Question 1044

Which of the following recovery strategies has the GREATEST chance of failure?

- ☐ Hot site
- ☐ Redundant site
- ☐ Reciprocal arrangement
- ☐ Cold site

Question 1045

Which program element should be implemented FIRST in asset classification and control?

- ☐ Risk assessment
- ☐ Classification
- ☐ Valuation
- ☐ Risk mitigation

Question 1046

The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

- ☐ sales department.
- ☐ database administrator.
- ☐ chief information officer (CIO).
- ☐ head of the sales department.

Question 1047

The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

- ☐ uses multiple redirects for completing a data commit transaction.
- ☐ has implemented cookies as the sole authentication mechanism.
- ☐ has been installed with a non-legitimate license key.
- ☐ is hosted on a server along with other applications.

Question 1048

Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

- ☐ Gantt chart
- ☐ Waterfall chart
- ☐ Critical path
- ☐ Rapid Application Development (RAD)

Question 1049

Which of the following is the PRIMARY responsibility of the information security manager when an organization implements the use of personally-owned devices on the corporate network?

- ☐ Requiring remote wipe capabilities
- ☐ Enforcing defined policy and procedures
- ☐ Conducting security awareness training
- ☐ Encrypting the data on mobile devices

Question 1050

Which of the following is a security manager's FIRST priority after an organization's critical system has been compromised?

- ☐ Implement improvements to prevent recurrence.
- ☐ Restore the compromised system.
- ☐ Preserve incident-related data.
- ☐ Identify the malware that compromised the system.

Question 1051

At the conclusion of a disaster recovery test, which of the following should ALWAYS be performed prior to leaving the vendor's hot site facility?

- ☐ Erase data and software from devices
- ☐ Conduct a meeting to evaluate the test
- ☐ Complete an assessment of the hot site provider
- ☐ Evaluate the results from all test scripts

Question 1052

The MOST important element in achieving executive commitment to an information security governance program is:

- ☐ a defined security framework
- ☐ identified business drivers
- ☐ established security strategies
- ☐ a process improvement model

Question 1053

An organization utilizes a third party to classify its customers' personally identifiable information (PII). What is the BEST way to hold the third party accountable for data leaks?

- ☐ Include detailed documentation requirements within the formal statement of work.
- ☐ Submit a formal request for proposal (RFP) containing detailed documentation of requirements.
- ☐ Ensure a nondisclosure agreement is signed by both parties' senior management.
- ☐ Require the service provider to sign off on the organization's acceptable use policy.

Question 1054

An organization plans to allow employees to use their own devices on the organization's network. Which of the following is the information security manager's BEST course of action?

- ☐ Implement automated software
- ☐ Assess associated risk
- ☐ Conduct awareness training
- ☐ Update the security policy

Question 1055

Which of the following is the MOST practical control that an organization can implement to prevent unauthorized downloading of data to universal serial bus (USB) storage devices?

- ☐ Two-factor authentication
- ☐ Restrict drive usage
- ☐ Strong encryption
- ☐ Disciplinary action

Question 1056

Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

- ☐ Ensure that all IT risks are identified
- ☐ Evaluate the impact of information security risks
- ☐ Demonstrate that IT mitigating controls are in place
- ☐ Suggest new IT controls to mitigate operational risk

Question 1057

Which of the following is the MOST effective way for senior management to support the integration of information security governance into corporate governance?

- ☐ Develop the information security strategy based on the enterprise strategy.
- ☐ Appoint a business manager as heard of information security.
- ☐ Promote organization-wide information security awareness campaigns.
- ☐ Establish a steering committee with representation from across the organization.

Question 1058

An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the BEST course of action for the information security manager?

- ☐ Present a business case for additional controls to senior management.
- ☐ Instruct IT to deploy controls based on urgent business needs.
- ☐ Solicit bids for compensating control products.
- ☐ Recommend a different application.

Question 1059

A large organization is considering a policy that would allow employees to bring their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

- ☐ higher costs in supporting end users
- ☐ impact on network capacity
- ☐ decrease in end user productivity
- ☐ lack of a device management solution

Question 1060

Of the following, which is the MOST important aspect of forensic investigations?

- ☐ The independence of the investigator
- ☐ Timely intervention
- ☐ Identifying the perpetrator
- ☐ Chain of custody

Question 1061

An organization finds unauthorized software has been installed on a number of workstations. The software was found to contain a Trojan which had been uploading data to an unknown external party. Which of the following would have BEST prevented the installation of the unauthorized software?

- ☐ Implementing application blacklisting
- ☐ Implementing an intrusion detection system (IDS)
- ☐ Banning executable file downloads at the Internet firewall
- ☐ Removing local administrator rights

Question 1062

Which of the following is the BEST indicator of a successful external intrusion into computer systems?

- ☐ Unexpected use of protocols within the DMZ.
- ☐ Unexpected increase of malformed URLs.
- ☐ Decrease in the number of login failures.
- ☐ Spikes in the number of login failures.

Question 1063

Which of the following is the PRIMARY purpose of establishing an information security governance framework?

- ☐ To minimize security risks
- ☐ To proactively address security objectives
- ☐ To reduce security audit issues
- ☐ To enhance business continuity planning

Question 1064

Which of the following situations would MOST inhibit the effective implementation of security governance?

- ☐ The complexity of technology
- ☐ Budgetary constraints
- ☐ Conflicting business priorities
- ☐ High-level sponsorship

Question 1065

A risk analysis should:

- ☐ include a benchmark of similar companies in its scope.
- ☐ assume an equal degree of protection for all assets.
- ☐ address the potential size and likelihood of loss.
- ☐ give more weight to the likelihood vs. the size of the loss.

Question 1066

The PRIMARY goal of information security governance to an organization is to:

- ☐ align with business processes
- ☐ align with business objectives
- ☐ establish a security strategy
- ☐ manage security costs

Question 1067

What is the PRIMARY objective of a post-event review in incident response?

- ☐ Adjust budget provisioning
- ☐ Preserve forensic data
- ☐ Improve the response process
- ☐ Ensure the incident is fully documented

Question 1068

When selecting risk response options to manage risk, an information security manager's MAIN focus should be on reducing:

- ☐ exposure to meet risk tolerance levels.
- ☐ the likelihood of threat.
- ☐ financial loss by transferring risk.
- ☐ the number of security vulnerabilities.

Question 1069

A major trading partner with access to the internal network is unwilling or unable to remediate serious information security exposures within its environment. Which of the following is the BEST recommendation?

- ☐ Sign a legal agreement assigning them all liability for any breach
- ☐ Remove all trading partner access until the situation improves
- ☐ Set up firewall rules restricting network traffic from that location
- ☐ Send periodic reminders advising them of their noncompliance

Question 1070

Information security governance is PRIMARILY driven by:

- ☐ technology constraints.
- ☐ regulatory requirements.
- ☐ litigation potential.
- ☐ business strategy.

Question 1071

Which of the following is the MOST effective at preventing an unauthorized individual from following an authorized person through a secured entrance (tailgating or piggybacking)?

- ☐ Card-key door locks
- ☐ Photo identification
- ☐ Biometric scanners
- ☐ Awareness training

Question 1072

Which of the following would be the FIRST step in establishing an information security program?

- ☐ Develop the security policy.
- ☐ Develop security operating procedures.
- ☐ Develop the security plan.
- ☐ Conduct a security controls study.

Question 1073

An information security manager has determined that the mean time to prioritize information security incidents has increased to an unacceptable level. Which of the following processes would BEST enable the information security manager to address this concern?

- ☐ Incident classification
- ☐ Vulnerability assessment
- ☐ Incident response
- ☐ Forensic analysis

Question 1074

Which of the following is the BEST performed by the security department?

- ☐ Approving standards for accessing the operating system
- ☐ Logging unauthorized access to the operating system
- ☐ Managing user profiles for accessing the operating system
- ☐ Provisioning users to access the operating system

Question 1075

Which of the following is the MOST important management signoff for migrating an order processing system from a test environment to a production environment?

- ☐ User
- ☐ Security
- ☐ Operations
- ☐ Database

Question 1076

When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

- ☐ The firewall should block all inbound traffic during the outage
- ☐ All systems should block new logins until the problem is corrected
- ☐ Access control should fall back to no synchronized mode
- ☐ System logs should record all user activity for later analysis

Question 1077

The PRIMARY advantage of single sign-on (SSO) is that it will:

- ☐ support multiple authentication mechanisms.
- ☐ increase the security related applications.
- ☐ strengthen user password.
- ☐ increase efficiency of access management.

Question 1078

To implement a security framework, an information security manager must FIRST develop:

- ☐ security standards.
- ☐ security procedures.
- ☐ a security policy.
- ☐ security guidelines.

Question 1079

Which of the following are the essential ingredients of a business impact analysis (BIA)?

- ☐ Downtime tolerance, resources and criticality
- ☐ Cost of business outages in a year as a factor of the security budget
- ☐ Business continuity testing methodology being deployed
- ☐ Structure of the crisis management team

Question 1080

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following MUST be in place for this solution to be relevant to the organization?

- ☐ Senior management support
- ☐ A data classification schema
- ☐ An adequate data testing environment
- ☐ A business case

Question 1081

Which of the following processes can be used to remediate identified technical vulnerabilities?

- ☐ Running baseline configurations
- ☐ Conducting a risk assessment
- ☐ Performing a business impact analysis (BIA)
- ☐ Running automated scanners

Question 1082

Which of the following would be the MOST effective countermeasure against malicious programming that rounds down transaction amounts and transfers them to the perpetrator's account?

- ☐ Ensure that proper controls exist for code review and release management
- ☐ Set up an agent to run a virus-scanning program across platforms
- ☐ Implement controls for continuous monitoring of middleware transactions
- ☐ Apply the latest patch programs to the production operating systems

Question 1083

Without prior approval, a training department enrolled the company in a free cloud-based collaboration site and invited employees to use it. Which of the following is the BEST response of the information security manager?

- ☐ Conduct a risk assessment and develop an impact analysis.
- ☐ Update the risk register and review the information security strategy.
- ☐ Report the activity to senior management.
- ☐ Allow temporary use of the site and monitor for data leakage.

Question 1084

What is the MOST important element to include when developing user security awareness material?

- ☐ Information regarding social engineering
- ☐ Detailed security policies
- ☐ Senior management endorsement
- ☐ Easy-to-read and compelling information

Question 1085

Which of the following is MOST effective in protecting against the attack technique known as phishing?

- ☐ Firewall blocking rules
- ☐ Up-to-date signature files
- ☐ Security awareness training
- ☐ Intrusion detection monitoring

Question 1086

For an organization that provides web-based services, which of the following security events would MOST likely initiate an incident response plan and be escalated to management?

- ☐ Multiple failed login attempts on an employee's workstation
- ☐ Suspicious network traffic originating from the demilitarized zone (DMZ)
- ☐ Several port scans of the web server
- ☐ Anti-malware alerts on several employees' workstations

Question 1087

Which of the following is the MOST effective method of preventing deliberate internal security breaches?

- ☐ Screening prospective employees
- ☐ Well-designed firewall system
- ☐ Well-designed intrusion detection system (IDS)
- ☐ Biometric security access control

Question 1088

Which of the following is the BEST way to verify that all critical production servers are utilizing up-to-date virus signature files?

- ☐ Verify the date that signature files were last pushed out
- ☐ Use a recently identified benign virus to test if it is quarantined
- ☐ Research the most recent signature file and compare to the console
- ☐ Check a sample of servers that the signature files are current

Question 1089

The PRIMARY reason for using information security metrics is to:

- ☐ achieve senior management commitment.
- ☐ ensure alignment with corporate requirements.
- ☐ adhere to legal and regulatory requirements.
- ☐ monitor the effectiveness of controls.

Question 1090

An organization with a strict need-to-know information access policy is about to launch a knowledge management intranet.

Which of the following is the MOST important activity to ensure compliance with existing security policies?

- ☐ Develop a control procedure to check content before it is published.
- ☐ Change organization policy to allow wider use of the new web site.
- ☐ Ensure that access to the web site is limited to senior managers and the board.
- ☐ Password-protect documents that contain confidential information.

Question 1091

The value of information assets is BEST determined by:

- ☐ individual business managers.
- ☐ business systems analysts.
- ☐ information security management.
- ☐ industry averages benchmarking.

Question 1092

Which of the following environments represents the GREATEST risk to organizational security?

- ☐ Locally managed file server
- ☐ Enterprise data warehouse
- ☐ Load-balanced, web server cluster
- ☐ Centrally managed data switch

Question 1093

What is the FIRST action an information security manager should take when a company laptop is reported stolen?

- ☐ Evaluate the impact of the information loss
- ☐ Update the corporate laptop inventory
- ☐ Ensure compliance with reporting procedures
- ☐ Disable the user account immediately

Question 1094

In a large organization, defining recovery time objectives (RTOs) is PRIMARILY the responsibility of:

- ☐ the IT manager.
- ☐ the information security manager.
- ☐ the business unit manager.
- ☐ senior manager.

Question 1095

Reviewing which of the following would BEST ensure that security controls are effective?

- ☐ Risk assessment policies
- ☐ Return on security investment
- ☐ Security metrics
- ☐ User access rights

Question 1096

A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

- ☐ Prepare an impact assessment report.
- ☐ Conduct a penetration test.
- ☐ Obtain approval from senior management.
- ☐ Back up the firewall configuration and policy files.

Question 1097

An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

- ☐ Intrusion detection system
- ☐ SIEM tool
- ☐ Antivirus software
- ☐ File integrity monitoring software

Question 1098

Most security vulnerabilities in software exist because:

- ☐ security features are not tested adequately.
- ☐ software has undocumented features.
- ☐ security is not properly designed.
- ☐ software is developed without adherence to standards.

Question 1099

The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

- ☐ ensure the confidentiality of sensitive material.
- ☐ provide a high assurance of identity.
- ☐ allow deployment of the active directory.
- ☐ implement secure sockets layer (SSL) encryption.

Question 1100

An information security manager determines the organization's critical systems may be vulnerable to a new zero-day attack. The FIRST course of action is to:

- ☐ advise management of risk and remediation cost.
- ☐ analyze the probability of compromise.
- ☐ survey peer organizations to see how they have addressed the issue.
- ☐ re-assess the firewall configuration.

Question 1101

Which of the following helps to ensure that the appropriate resources are applied in a timely manner after an incident has occurred?

- ☐ Initiate an incident management log.
- ☐ Define incident response teams.
- ☐ Broadcast an emergency message.
- ☐ Classify the incident.

Question 1102

When developing security processes for handling credit card data on the business unit's information system, the information security manager should FIRST:

- ☐ review corporate policies regarding credit card information.
- ☐ implement the credit card companies' security requirements.
- ☐ ensure that systems handle credit card data are segmented.
- ☐ review industry's best practices for handling secure payments.

Question 1103

The BEST way to mitigate the risk associated with a social engineering attack is to:

- ☐ deploy an effective intrusion detection system (IDS)
- ☐ perform a user-knowledge gap assessment of information security practices
- ☐ perform a business risk assessment of the email filtering system
- ☐ implement multi-factor authentication on critical business systems

Question 1104

For an enterprise implementing a bring your own device (BYOD) program, which of the following would provide the BEST security of corporate data residing on unsecured mobile devices?

- ☐ Acceptable use policy
- ☐ Device certification process
- ☐ Containerization solution
- ☐ Data loss prevention (DLP)

Question 1105

When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:

- ☐ aligned with the IT strategic plan.
- ☐ based on the current rate of technological change.
- ☐ three-to-five years for both hardware and software.
- ☐ aligned with the business strategy.

Question 1106

The MOST important success factor to design an effective IT security awareness program is to:

- ☐ customize the content to the target audience.
- ☐ ensure senior management is represented.
- ☐ ensure that all the staff is trained.
- ☐ avoid technical content but give concrete examples.

Question 1107

Nonrepudiation can BEST be assured by using:

- ☐ delivery path tracing.
- ☐ reverse lookup translation.
- ☐ out-of-hand channels.
- ☐ digital signatures.

Question 1108

Which of the following is the BEST way to integrate information security into corporate governance?

- ☐ Engage external security consultants in security initiatives.
- ☐ Conduct comprehensive information security management training for key stakeholders.
- ☐ Ensure information security processes are part of the existing management processes.
- ☐ Require periodic security risk assessments be performed.

Question 1109

What is the BEST way to ensure users comply with organizational security requirements for password complexity?

- ☐ Include password construction requirements in the security standards
- ☐ Require each user to acknowledge the password requirements
- ☐ Implement strict penalties for user noncompliance
- ☐ Enable system-enforced password configuration

Question 1110

Which of the following approaches is BEST for selecting controls to minimize information security risks?

- ☐ Cost-benefit analysis
- ☐ Control-effectiveness
- ☐ Risk assessment
- ☐ Industry best practices

Question 1111

Which of the following represents the MAJOR focus of privacy regulations?

- ☐ Unrestricted data mining
- ☐ Identity theft
- ☐ Human rights protection D.
- ☐ Identifiable personal data

Question 1112

Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

- ☐ Continuous analysis, monitoring and feedback
- ☐ Continuous monitoring of the return on security investment (ROSD)
- ☐ Continuous risk reduction
- ☐ Key risk indicator (KRD) setup to security management processes

Question 1113

Which of the following is the BEST defense against a brute force attack?

- ☐ Discretionary access control
- ☐ Intruder detection lockout
- ☐ Time-of-day restrictions
- ☐ Mandatory access control

Question 1114

Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

- ☐ Historical cost of the asset
- ☐ Acceptable level of potential business impacts
- ☐ Cost versus benefit of additional mitigating controls
- ☐ Annualized loss expectancy (ALE)

Question 1115

Which of the following is MOST important in developing a security strategy?

- ☐ Creating a positive business security environment
- ☐ Understanding key business objectives
- ☐ Having a reporting line to senior management
- ☐ Allocating sufficient resources to information security

Question 1116

Acceptable risk is achieved when:

- ☐ residual risk is minimized.
- ☐ transferred risk is minimized.
- ☐ control risk is minimized.
- ☐ inherent risk is minimized.

Question 1117

Which of the following is an inherent weakness of signature-based intrusion detection systems?

- ☐ A higher number of false positives
- ☐ New attack methods will be missed
- ☐ Long duration probing will be missed
- ☐ Attack profiles can be easily spoofed

Question 1118

An information security manager that is utilizing a public cloud is performing a root cause investigation of an incident that took place in that environment. Which of the following should be the security manager's MAIN concern?

- ☐ Limited access to information
- ☐ Shared infrastructure with other subscribers
- ☐ Transaction records split into multiple cloud locations
- ☐ Lack of security log filtering

Question 1119

Which of the following would be the BEST way for an information security manager to justify ongoing annual maintenance fees associated with an intrusion prevention system (IPS)?

- ☐ Perform a penetration test to demonstrate the ability to protect.
- ☐ Perform industry research annually and document the overall ranking of the IPS.
- ☐ Establish and present appropriate metrics that track performance.
- ☐ Provide yearly competitive pricing to illustrate the value of the IPS.

Question 1120

Which of the following is the FIRST phase in which security should be addressed in the development cycle of a project?

- ☐ Design
- ☐ Implementation
- ☐ Application security testing
- ☐ Feasibility

Question 1121

An information security program should be sponsored by:

- ☐ infrastructure management.
- ☐ the corporate audit department.
- ☐ key business process owners.
- ☐ information security management.

Question 1122

The IT function has declared that, when putting a new application into production, it is not necessary to update the business impact analysis (BIA) because it does not produce modifications in the business processes. The information security manager should:

- ☐ verify the decision with the business units.
- ☐ check the system's risk analysis.
- ☐ recommend update after post implementation review.
- ☐ request an audit review.

Question 1123

After logging in to a web application, further password credentials are required at various application points. Which of the following is the PRIMARY reason for such an approach?

- ☐ To ensure access is granted to the authorized person
- ☐ To enforce strong two-factor authentication
- ☐ To ensure session management variables are secure
- ☐ To implement single sign-on

Question 1124

Which of the following will MOST effectively minimize the chance of inadvertent disclosure of confidential information?

- ☐ Following the principle of least privilege
- ☐ Restricting the use of removable media
- ☐ Applying data classification rules
- ☐ Enforcing penalties for security policy violations

Question 1125

When electronically stored information is requested during a fraud investigation, which of the following should be the FIRST priority?

- ☐ Assigning responsibility for acquiring the data
- ☐ Locating the data and preserving the integrity of the data
- ☐ Creating a forensically sound image
- ☐ Issuing a litigation hold to all affected parties

Question 1126

Which of the following metrics is the BEST indicator of an abuse of the change management process that could compromise information security?

- ☐ Small number of change request
- ☐ Large percentage decrease in monthly change requests
- ☐ Percentage of changes that include post-approval supplemental add-ons
- ☐ High ratio of lines of code changed to total lines of code

Question 1127

Which of the following is the MOST important element to ensure the success of a disaster recovery test at a vendor-provided hot site?

- ☐ Tests are scheduled on weekends
- ☐ Network IP addresses are predefined
- ☐ Equipment at the hot site is identical
- ☐ Business management actively participates

Question 1128

Which of the following is a potential indicator of inappropriate Internet use by staff?

- ☐ Increased help desk calls for password resets
- ☐ Reduced number of pings on firewalls
- ☐ Increased reports of slow system performance
- ☐ Increased number of weakness from vulnerability scans

Question 1129

Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

- ☐ Regular review of access control lists
- ☐ Security guard escort of visitors
- ☐ Visitor registry log at the door
- ☐ A biometric coupled with a PIN

Question 1130

A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

- ☐ Representation by regional business leaders
- ☐ Composition of the board
- ☐ Cultures of the different countries
- ☐ IT security skills

Question 1131

Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

- ☐ Platform security
- ☐ Entitlement changes
- ☐ Intrusion detection
- ☐ Antivirus controls

Question 1132

Failure to include information security requirements within the build/buy decision would MOST likely result in the need for:

- ☐ compensating controls in the operational environment.
- ☐ commercial product compliance with corporate standards.
- ☐ more stringent source programming standards.
- ☐ security scanning of operational platforms.

Question 1133

Which of the following is the MOST significant advantage of developing a well-defined information security strategy?

- ☐ Support for buy-in from organizational employees
- ☐ Allocation of resources to highest priorities
- ☐ Prevention of deviations from risk tolerance thresholds
- ☐ Increased maturity of incident response processes

Question 1134

Which of the following is MOST important in determining whether a disaster recovery test is successful?

- ☐ Only business data files from offsite storage are used
- ☐ IT staff fully recovers the processing infrastructure
- ☐ Critical business processes are duplicated
- ☐ All systems are restored within recovery time objectives (RTOs)

Question 1135

An organization's outsourced firewall was poorly configured and allowed unauthorized access that resulted in downtime of 48 hours. Which of the following should be the information security manager's NEXT course of action?

- ☐ Reconfigure the firewall in accordance with best practices.
- ☐ Obtain supporting evidence that the problem has been corrected.
- ☐ Revisit the contract and improve accountability of the service provider.
- ☐ Seek damages from the service provider.

Question 1136

Which of the following BEST contributes to the successful management of security incidents?

- ☐ Established procedures
- ☐ Established policies
- ☐ Tested controls
- ☐ Current technologies

Question 1137

After detecting an advanced persistent threat (APT), which of the following should be the information security manager's FIRST step?

- ☐ Notify management
- ☐ Contain the threat
- ☐ Remove the threat
- ☐ Perform root-cause analysis

Question 1138

Which of the following is the MOST serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 p.m. (23.00 hrs.)?

- ☐ Most new viruses* signatures are identified over weekends
- ☐ Technical personnel are not available to support the operation
- ☐ Systems are vulnerable to new viruses during the intervening week
- ☐ The update's success or failure is not known until Monday

Question 1139

Which of the following would BEST help to ensure the alignment between information security and business functions?

- ☐ Developing information security policies
- ☐ Establishing an information security governance committee
- ☐ Establishing a security awareness program
- ☐ Providing funding for information security efforts

Question 1140

Developing a successful business case for the acquisition of information security software products can BEST be assisted by:

- ☐ assessing the frequency of incidents.
- ☐ quantifying the cost of control failures.
- ☐ calculating return on investment (ROI) projections.
- ☐ comparing spending against similar organizations.

Question 1141

Which of the following is the PRIMARY goal of business continuity management?

- ☐ Establish incident response procedures.
- ☐ Assess the impact to business processes.
- ☐ Increase survivability of the organization.
- ☐ Implement controls to prevent disaster.

Question 1142

The MOST important component of a privacy policy is:

- ☐ notifications.
- ☐ warranties.
- ☐ liabilities.
- ☐ geographic coverage.

Question 1143

In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

- ☐ original cost to acquire.
- ☐ cost of the software stored.
- ☐ annualized loss expectancy (ALE).
- ☐ cost to obtain a replacement.

Question 1144

An organization is considering moving one of its critical business applications to a cloud hosting service. The cloud provider may not provide the same level of security for this application as the organization. Which of the following will provide the BEST information to help maintain the security posture?

- ☐ Risk assessment
- ☐ Cloud security strategy
- ☐ Vulnerability assessment
- ☐ Risk governance framework

Question 1145

An information security manager is preparing a presentation to obtain support for a security initiative. Which of the following would be the BEST way to obtain management's commitment for the initiative?

- ☐ Include historical data of reported incidents
- ☐ Provide the estimated return on investment
- ☐ Provide an analysis of current risk exposures
- ☐ Include industry benchmarking comparisons

Question 1146

For risk management purposes, the value of an asset should be based on:

- ☐ original cost.
- ☐ net cash flow.
- ☐ net present value.
- ☐ replacement cost.

Question 1147

The BEST way to ensure that information security policies are followed is to:

- ☐ distribute printed copies to all employees.
- ☐ perform periodic reviews for compliance.
- ☐ include escalating penalties for noncompliance.
- ☐ establish an anonymous hotline to report policy abuses.

Question 1148

Security monitoring mechanisms should PRIMARILY:

- ☐ focus on business-critical information.
- ☐ assist owners to manage control risks.
- ☐ focus on detecting network intrusions.
- ☐ record all security violations.

Question 1149

A software vendor has announced a zero-day vulnerability that exposes an organization's critical business systems, following should be the information security manager's PRIMARY concern?

- ☐ Business tolerance of downtime
- ☐ Adequacy of the incident response plan
- ☐ Availability of resources to implement controls
- ☐ Ability to test patches prior to deployment

Question 1150

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized disclosure?

- ☐ Authenticity
- ☐ Confidentiality
- ☐ Nonrepudiation
- ☐ Integrity

Question 1151

Which of the following would provide the MOST essential input for the development of an information security strategy?

- ☐ Measurement of security performance against IT goals
- ☐ Results of an information security gap analysis
- ☐ Availability of capable information security resources
- ☐ Results of a technology risk assessment

Question 1152

Which of the following is the MOST effective way to communicate information security risk to senior management?

- ☐ Business impact analysis
- ☐ Balanced scorecard
- ☐ Key performance indicators (KPIs)
- ☐ Heat map

Question 1153

A risk mitigation report would include recommendations for:

- ☐ assessment.
- ☐ acceptance.
- ☐ evaluation.
- ☐ quantification.

Question 1154

An organization has decided to conduct a postmortem analysis after experiencing a loss from an information security attack. The PRIMARY purpose of this analysis should be to:

- ☐ prepare for criminal prosecution.
- ☐ document lessons learned.
- ☐ evaluate the impact.
- ☐ update information security policies.